

高等学校**应用型特色**规划教材

计算机网络信息安全

刘永华　主　编
陈　茜　张淑玉　周金玲　副主编

赠送
电子教案

清华大学出版社

高等学校应用型特色规划教材

计算机网络信息安全

刘永华　主　编

陈茜　张淑玉　周金玲　副主编

清华大学出版社
北　京

内 容 简 介

本书的内容涵盖了计算机网络安全和管理的基本概念、原理和技术，全书共分为 10 章。主要内容包括计算机网络安全概述、数据加密与认证技术、操作系统安全技术、数据库与数据安全技术、计算机病毒防治技术、防火墙技术、入侵检测技术、VPN 与 NAT 技术及安全协议、计算机网络管理与维护技术、网络信息安全系统设计案例等内容。本书内容全面，取材新颖，既有网络安全和管理的理论知识，又有应用案例和实用技术，反映了计算机网络信息安全技术的最新发展。

本书可作为普通高等教育和成人高等教育计算机科学与技术、网络工程、软件工程、通信工程、自动化及相关专业本科教材使用，也可作为高职高专计算机网络安全技术教材使用，同时也是广大工程技术人员较好的科技参考书。

图书在版编目(CIP)数据

计算机网络信息安全/刘永华主编. --北京：清华大学出版社，2014
(高等学校应用型特色规划教材)
ISBN 978-7-302-35623-3

Ⅰ. ①计…　Ⅱ. ①刘…　Ⅲ. ①计算机网络—信息安全—高等学校—教材　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2014)第 046701 号

责任编辑：桑任松
封面设计：杨玉兰
责任校对：周剑云
责任印制：

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn, http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015, zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn, 010-62791865
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张：**19.75　　**字　数：**477 千字
版　　次：2014 年 7 月第 1 版　　**印　次：**2014 年 7 月第 1 次印刷
印　　数：1～3000
定　　价：36.00 元

产品编号：050543-01

前　　言

计算机网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠地运行，网络服务不中断。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。随着计算机网络技术的发展，网络的安全问题越来越受到关注，网络安全已超越其本身而达到国家安全的高度。

本书在介绍网络安全理论及其基础知识的同时，突出计算机网络安全方面的管理、配置及维护的实际操作手法和手段，并尽量跟踪网络安全技术的最新成果与发展方向，结合网络安全系统案例精心阐述。全书主要内容包括网络安全的基本概念、数据加密与认证技术、操作系统的安全与保护措施、数据库与数据安全、防火墙技术、黑客技术与防范措施、网络病毒技术、VPN 技术与安全协议、网络管理与维护技术、Internet/Intranet 的安全性、网络信息安全系统案例等。

全书共分为 10 章，各章内容安排如下。

第 1 章具体介绍计算机网络安全的相关基础知识，包括网络安全的概念及影响网络安全的主要因素，网络安全的组成以及网络安全常用的技术；第 2 章介绍网络安全中数据加密与认证技术，包括传统的加密方法、DES 加密标准、公开密钥体制和数字签名等技术；第 3 章主要介绍操作系统安全技术，包括 Windows 和 Linux 操作系统的安全机制、安全漏洞和安全配置方案；第 4 章介绍数据库与数据安全技术, 数据库的安全特性、数据库的安全、保护数据的完整性、数据备份和恢复、网络备份、系统数据容灾等；第 5 章主要介绍病毒的原理、病毒的类型和计算机网络病毒，同时介绍了几种影响较大的网络病毒，并且介绍了病毒的清除及防护措施；第 6 章介绍访问控制技术中的防火墙的技术，包括防火墙的原理、种类和实现策略等；第 7 章主要介绍对入侵检测的概念和相关技术进行了全面介绍，并对入侵检测的未来发展进行了讨论；第 8 章主要介绍了 VPN 与 NAT 技术及安全协议，涉及 VPN 的原理与设置、NAT 的工作工程，以及网络安全的几个主要协议；第 9 章主要介绍计算机网络管理和维护技术。主要包括网络管理的基本概念、网络管理协议、网络管理工具和网络维护方法。介绍 Windows 自带的常用网络工具，讨论了网卡、集线器、交换机、路由器、网线和 RJ-45 接头等网络连接设备的维护，网络的性能优化等问题，重点介绍了常用网络故障及排除方法；第 10 章主要介绍网络信息安全系统设计案例。涉及需求分析、工程论证、总体设计与实体设计等内容。

由于网络安全的内容非常丰富，本书按理论教学以“必需、够用”为度，加强实践性环节教学，提高学生的实际技能的原则组织编写。讲究知识性、系统性、条理性、连贯性。力求激发学生兴趣，注重提示各知识之间的内在联系，精心组织内容，做到由浅入深，由易到难，删繁就简，突出重点，循序渐进。本书既注重网络安全基础理论，又着眼培养读者解决网络安全问题的能力。

本书的特点是文字简明、图表准确、通俗易懂，用循序渐进的方式叙述网络安全知识，对计算机网络安全的原理和技术难点的介绍适度，内容安排合理，逻辑性强，重点介绍网



络安全的概念、技术和应用，在内容上将理论知识和实际应用紧密地结合在一起。本书共10 章，适用于 48 学时左右的课堂教学。通过对本书的学习，可使读者较全面地了解网络系统安全的基本概念、网络安全技术和应用，培养读者解决网络安全问题的能力。

本书可作为普通高等教育和成人高等教育计算机科学与技术、网络工程、软件工程、通信工程、自动化及相关专业本科教材使用，也可作为高职高专计算机网络安全技术教材使用，同时也是广大工程技术人员较好的科技参考书。

本书由刘永华担任主编并完成全书的通稿整理，陈茜、张淑玉、周金玲担任副主编。其中第 1～7 章由刘永华编写，第 8 章由陈茜编写，第 9 章由张淑玉编写，第 10 章由董春平编写。孟凡楼、孙俊香、赵艳杰、解圣庆、周建梁、张宗云对本书的编写提供了帮助，在此向他们表示感谢。

由于作者水平有限，加之编写时间仓促，书中难免有疏漏和不足之处，恳请广大读者和同行批评指正。

编　者

目　　录





第 1 章　计算机网络安全概述

学习目标

系统学习网络安全的概念，网络安全的现状，网络面临的主要威胁，影响网络安全的因素，保证网络安全的技术。通过本章的学习，读者应掌握及了解以下内容。

- 掌握网络安全的概念，网络安全的基本技术。
- 了解网络的安全威胁，影响网络安全的主要因素。

1.1　计算机网络安全简介

随着信息技术的迅速发展，网络已成为重要的信息传播工具。而随着互联网的飞速发展，网络安全问题也越来越受到广泛的关注，各种病毒花样繁多、层出不穷，系统、程序、软件的安全漏洞越来越多，黑客们常通过不正当手段侵入他人计算机，非法获得用户信息资料，给正常使用互联网的用户带来不可估计的损失。因此，网络安全越来越引起人们的重视。

1.1.1　网络安全的概念

人们在享受信息化带来的众多好处的同时，也面临着日益突出的信息安全与保密的问题。计算机网络信息安全技术经过 10 多年的发展，在信息安全技术的研究基础上形成了两个完全不同的角度和方向：一个从正面防御角度考虑，研究加密、鉴别、认证、授权和访问控制等；另一个从反面攻击角度考虑，研究漏洞的扫描评估、入侵检测、紧急响应和病毒预防。网络安全从其本质上来讲就是网络上的信息安全。它涉及的领域相当广泛，这是因为在目前的公用通信网络中存在着各种各样的安全漏洞和威胁。下面给出网络安全的一个通用定义。

网络安全就是网络上的信息安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统能连续、可靠正常地运行，使网络服务不中断。

广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全所要研究的领域。

网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两者相互补充，缺一不可。技术方面主要侧重于防范外部非法用户的攻击，管理方面则侧重于内部人为因素的管理。

网络安全要考虑以下几个方面的内容。

1. 网络系统的安全

网络系统的安全主要包括以下几方面的问题。

(1)　网络操作系统的安全性。目前流行的操作系统(UNIX、Windows 2000/ NT/XP 等)



均存在网络安全漏洞。

(2) 来自外部的安全威胁。

(3) 来自内部用户的安全威胁。

(4) 通信协议软件本身缺乏安全性(如 TCP/IP 协议)。

(5) 计算机病毒感染。

(6) 应用服务的安全。许多应用服务系统在访问控制及安全通信方面考虑不周全。

2. 局域网安全

局域网采用广播方式，在同一个广播域中可以侦听到在该局域网上传输的所有信息包，这是一个不安全的因素。

3. Internet 互联安全

非授权访问、冒充合法用户、破坏数据完整性、干扰系统正常运行、利用网络传播病毒等都是在 Internet 上经常遇到的问题。

4. 数据安全

事实上，无论 Internet 还是其他专用网络，都必须注意数据的安全性问题，以保护本单位、本部门的信息资源不会受到外来的侵害。

从根本意义上讲，绝对安全的计算机是根本不存在的，绝对安全的网络也是不可能有的。只有存放在一个无人知晓的密室里，而又不通电的计算机才可以称得上安全。计算机只要投入使用，就或多或少地存在着安全问题，只是程度不同而已。因此，在探讨网络安全的时候，实际上指的是一定程度上的网络安全。而到底需要多大的安全性，要依据实际需要及自身能力而定。网络安全性越高，也就意味着网络的管理越复杂。网络的安全性与网络管理便利性是一对矛盾。

1.1.2 网络安全模型

典型的网络安全模型如图 1.1 所示。信息需要从一方通过网络传送到另一方。在传送中居主体地位的双方必须相互合作以便进行交换。通过通信协议(如 TCP/IP)在两个主体之间可以建立一条逻辑信息通道。

为防止对手对信息机密性、可靠性等造成破坏，需要保护传送的信息。保证安全性的所有机制包括以下两部分。

(1) 对被传送的信息进行与安全相关的转换。图 1.1 中包含了加密消息和以消息内容为基础的补充代码。加密消息使对手无法阅读，补充代码可以用来验证发送方的身份。

(2) 两个主体共享不希望对手得知的保密信息。例如，使用密钥链接，在发送前对信息进行转换，在接收后再转换回来。

为了实现安全传送，可能需要可信任的第三方。例如，第三方可能会负责向两个主体分发保密信息，而向其他对手保密，或者需要第三方对两个主体间传送信息可靠性的争端进行仲裁。

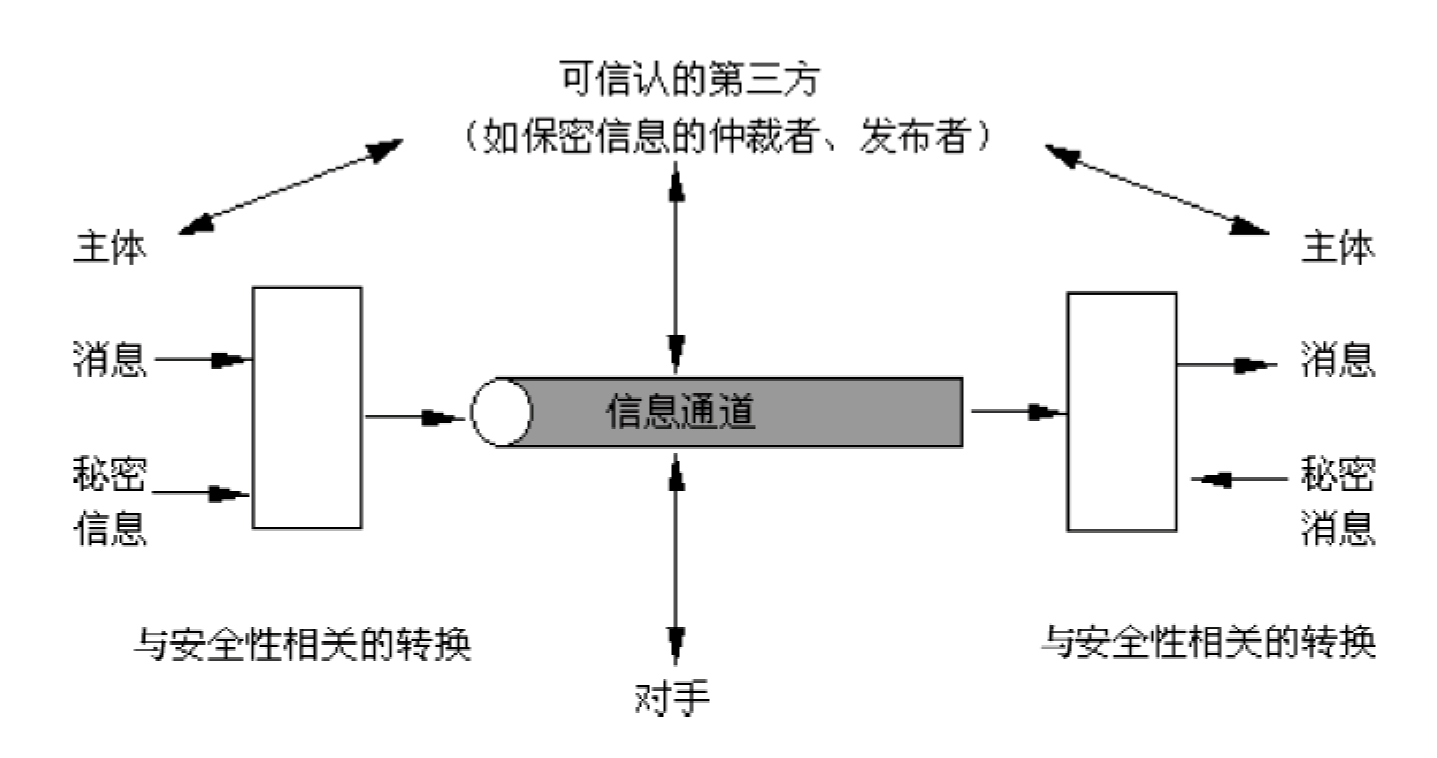


图 1.1　网络安全模型

这种通用模型指出了设计特定安全服务的 4 个基本任务。

(1) 设计执行与安全性相关的转换算法，该算法必须使对手不能对算法进行破解以实现其目的。

(2) 生成算法使用的保密信息。

(3) 开发分发和共享保密信息的方法。

(4) 指定两个主体要使用的协议，并利用安全算法和保密信息来实现特定的安全服务。

1.1.3　计算机安全的分级

计算机操作系统的安全级别在美国国防部发表的橘皮书——《可信计算机系统评测标准》中，把计算机系统分为 4 个等级、7 个级别，即 D(最低保护等级)、C(自主保护等级)、B(强制保护等级)、A(验证保护等级)4 等，细分为 D、C1、C2、B1、B2、B3、A1 等 7 级。

- D 级。计算机安全的最低一级，不要求用户进行登录和密码保护，任何人都可以使用，整个系统是不可信任的，硬件和软件都易被他人侵袭。
- C1 级。自主安全保护级。要求硬件有一定的安全级(如计算机带锁)，用户必须通过登录认证方可使用系统，并建立了访问许可权限机制。
- C2 级。受控存取保护级。比 C1 级增加了几个特性，即：引进了受控访问环境，进一步限制了用户执行某些系统指令；授权分级使系统管理员给用户分组，授予他们访问某些程序和分级目录的权限；采用系统审计，跟踪记录所有安全事件及系统管理员的工作。
- B1 级。标记安全保护级。对网络上每个对象都给予实施保护；支持多级安全，对网络、应用程序工作站实施不同的安全策略；对象必须在访问控制之下，不允许拥有者自己改变所属资源的权限。
- B2 级。结构化保护级。对网络和计算机系统中所有对象都加以定义，分配给一个标签；为工作站、终端等设备分配不同的安全级别；按最小特权原则取消权力无限大的特权用户。
- B3 级。安全域级。要求用户工作站或终端必须通过可信任的途径链接到网络系统内部的主机上；采用硬件来保护系统的数据存储区；根据最小特权原则，增加了系统安全员，将系统管理员、系统操作员和系统安全员的职责分离，将人为因素对计算机安全的威胁降至最小。



- A1 级。验证设计级。这是计算机安全级别中最高的一级，本级包括了以上各级别的所有措施，并附加了一个安全系统的受监视设计；合格的个体必须经过分析并通过这一设计；所有构成系统的部件来源都必须有安全保证；这一级还规定了将安全计算机系统运送到现场安装所必须遵守的程序。

在网络的具体设计过程中，应根据网络总体规划中提出的各项技术规范、设备类型、性能要求及经费等，综合考虑来确定一个比较合理、性能较高的网络安全级别，从而实现网络的安全性和可靠性。

1.1.4　网络安全的重要性

在信息社会中，信息具有与能源、物源同等的价值，在某些时候甚至具有更高的价值。具有价值的信息必然存在安全性的问题，对于企业更是如此。例如，在竞争激烈的市场经济驱动下，每个企业对于原料配额、生产技术、经营决策等信息，在特定的地点和业务范围内都具有保密的要求，一旦这些机密被泄露，不仅会给企业，而且会给国家造成严重的经济损失。

经济社会的发展要求各用户之间的通信和资源共享，需要将一批计算机联成网络，这样就隐含着很大的风险，包含了极大的脆弱性和复杂性，特别是对当今最大的网络——Internet，很容易遭到别有用心者的恶意攻击和破坏。随着国民经济的信息化程度的提高，有关的大量情报和商务信息都高度集中地存放在计算机中，随着网络应用范围的扩大，信息的泄露问题也变得日益严重，因此，计算机网络的安全性问题就越来越重要。

1.2　计算机网络安全的现状

互联网与生俱有的开放性、交互性和分散性特征使人类所憧憬的信息共享、开放、灵活和快速等需求得到满足。网络环境为信息共享、信息交流、信息服务创造了理想空间，网络技术的迅速发展和广泛应用，为人类社会的进步提供了巨大推动力。正是由于互联网的上述特性，产生了许多安全问题。

(1) 黑客(Hacker)。这是指在 Internet 上有一批熟悉网络技术的人，经常利用网络上现存的一些漏洞，设法进入他人的计算机系统。有些人只是为了好奇，而有些人是心怀不良动机侵入他人系统，他们偷窥机密信息，或将其计算机系统破坏，这部分人就被称为“黑客”。尽管人们在计算机技术上做出了种种努力，但这种攻击却是愈演愈烈。从单一地利用计算机病毒破坏和用黑客手段进行入侵攻击转变为使用恶意代码与黑客攻击手段相结合，使得这种攻击具有传播速度迅猛、受害面惊人和穿透深度广的特点，往往一次攻击就会给受害者带来严重的破坏和损失。

(2) 信息泄露、信息污染、信息不易受控。例如，资源未授权侵用、未授权信息流出现、系统拒绝信息流和系统否认等，这些都是信息安全的技术难点。

(3) 在网络环境中，一些组织或个人出于某种特殊目的，进行信息泄密、信息破坏、信息侵权和意识形态的信息渗透，甚至通过网络进行政治颠覆等活动，使国家利益、社会公共利益和各类主体的合法权益受到威胁。

(4) 网络运用的趋势是全社会广泛参与，随之而来的是控制权分散的管理问题。由于

人们的利益、目标及价值观产生分歧，使信息资源的保护和管理出现脱节和真空，从而使信息安全问题变得广泛而复杂。

(5) 随着社会重要基础设施的高度信息化，社会的“命脉”和核心控制系统有可能面临恶意攻击而导致损坏和瘫痪，包括国防通信设施、动力控制网、金融系统和政府网站等。

近年来，人们的网络安全意识逐步提高，很多企业根据核心数据库和系统运营的需要，逐步部署了防火墙、防病毒和入侵监测系统等安全产品，并配备了相应的安全策略。虽然有了这些措施，但并不能解决一切问题。我国网络安全问题日益突出，其主要表现在以下几个方面。

1. 安全事件不能及时、准确发现

网络设备、安全设备、系统每天生成的日志可能有上万条甚至几十万条，这样人工地对多个安全系统的大量日志进行实时审计、分析流于形式，再加上误报(如网络入侵检测系统 NIDS、互联网协议群 IPS)、漏报(如未知病毒、未知网络攻击、未知系统攻击)等问题，造成不能及时、准确地发现安全事件。

2. 安全事件不能准确定位

信息安全系统通常是由防火墙、入侵检测、漏洞扫描、安全审计、防病毒、流量监控等产品组成的，但是由于安全产品来自不同的厂商，没有统一的标准，所以安全产品之间无法进行信息交流，于是形成许多安全孤岛和安全盲区。由于事件孤立，相互之间无法形成很好的集成关联，因而一个事件的出现不能关联到真实问题。

如入侵监测系统事件报警，就需关联同一时间防火墙报警、被攻击的服务器安全日志报警等，从而了解是真实报警还是误报；如是未知病毒的攻击，则分为两类，即网络病毒、主机病毒。网络病毒大都表现为流量异常，主机病毒大都表现为中央处理器异常、内存异常、磁盘空间异常、文件的属性和大小改变等。要发现这个问题，需要关联流量监控(网络病毒)、服务器运行状态监控(主机病毒)、完整性检测(主机病毒)来发现。为了预防网络病毒大规模爆发，则必须在病毒爆发前快速发现中毒机器并切断源头。如服务器的攻击，可能是安全事件遭病毒感染；分布式拒绝服务 DDoS(Distributed Denial of Service)攻击，可能是服务器 CPU 超负荷；端口某服务流量太大、访问量太大等，必须将多种因素结合起来才能更好地分析，快速知道真实问题点并及时恢复正常。

DDoS 是一种基于 DoS 的特殊形式的拒绝服务攻击，是一种分布、协作的大规模攻击方式，主要瞄准比较大的站点，像商业公司、搜索引擎和政府部门的站点。DDoS 攻击是利用一批受控制的机器向一台机器发起攻击，这样来势迅猛的攻击令人难以防备，因此具有较大的破坏性。

3. 无法做集中的事件自动统计

它包括某台服务器的安全情况报表、所有机房发生攻击事件的频率报表、网络中利用次数最多的攻击方式报表、发生攻击事件的网段报表、服务器性能利用率最低的服务器列表等。需要管理员人为地对这些事件做统计记录，生成报告，从而耗费大量人力。



4. 缺乏有效的事件处理查询

没有对事件处理的整个过程做跟踪记录，信息部门主管不了解哪些管理员对该事件进行了处理，对处理过程和结果也没有做记录，使得处理的知识和经验不能得到共享，导致下次再发生类似事件时，处理效率的低下。

5. 缺乏专业的安全技能

管理员发现问题后，往往因为安全知识的不足导致事件迟迟不能被处理，从而影响网络的安全性，延误网络的正常使用。

1.3 计算机网络安全威胁

安全威胁是指某个人、物、事件或概念对某一资源的机密性、完整性、可用性或合法性所造成的危害。某种攻击就是某种威胁的具体实现。

安全威胁可分为故意的(如黑客渗透)和偶然的(如信息被发往错误的地址)两类。故意威胁又可进一步分为被动和主动两类。

1.3.1 安全攻击

对于计算机或网络安全性的攻击，一般是通过在提供信息时查看计算机系统的功能来记录其特性。当信息从信源向信宿流动时，图 1.2 中列出了信息正常流动和受到各种类型的攻击的情况。

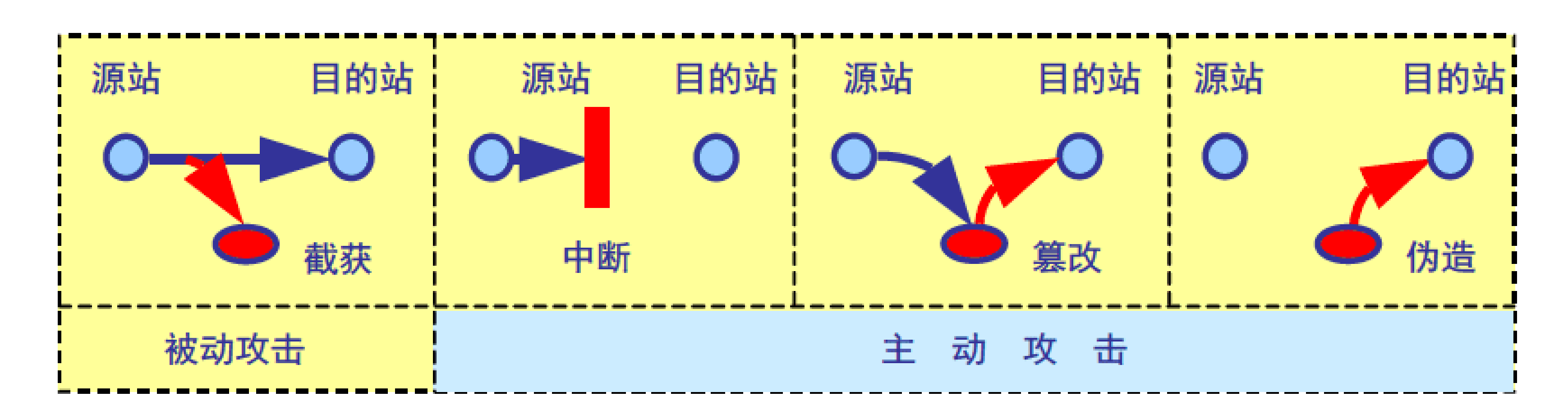


图 1.2 安全攻击

(1) 中断是指系统资源遭到破坏或变得不能使用。这是对可用性的攻击。例如，对一些硬件进行破坏、切断通信线路或禁用文件管理系统。

(2) 截获是指未授权的实体得到了资源的访问权，这是对保密性的攻击。未授权实体可能是一个人、一个程序或一台计算机。

(3) 篡改是指未授权的实体不仅得到了访问权，而且还篡改了资源，这是对完整性的攻击。

(4) 伪造是指未授权的实体向系统中插入伪造的对象，这是对真实性的攻击。

1. 被动攻击与主动攻击

以上这些攻击类型还可分为被动攻击和主动攻击两种，下面详细介绍。

(1) 被动攻击的特点是偷听或监视传送，其目的是获取正在传送的消息。被动攻击有泄露信息内容和通信量分析等。①泄露信息内容容易理解，包括电话对话、电子邮件消息

以及可能含有敏感的机密信息，要防止对手从传送中获得这些内容。②通信量分析则比较微妙，是用某种方法将信息内容隐藏起来，常用的技术是加密，这样即使对手捕获了消息，也不能从中提取信息。对手可以确定位置和通信主机的身份，可以观察交换消息的频率和长度。这些信息可以帮助对手猜测正在进行的通信特性。

(2) 主动攻击涉及修改数据或创建错误的数据流，它包括假冒、重放、修改消息和拒绝服务等。①假冒是一个实体假装成另一个实体，假冒攻击通常包括一种其他形式的主动攻击；②重放涉及被动捕获数据单元及其后来的重新传送，以产生未经授权的效果；③修改消息意味着改变了真实消息的部分内容，或将消息延迟或重新排序，导致未授权的操作；④拒绝服务是指禁止对通信工具的正常使用或管理，这种攻击拥有特定的目标；另一种拒绝服务的形式是整个网络的中断，可以通过使网络失效而实现，或通过消息过载使网络性能降低。主动攻击具有与被动攻击相反的特点。虽然很难检测出被动攻击，但可以采取措施防止它的成功。相反，很难绝对预防主动攻击，因为这样需要随时对所有的通信工具和路径进行完全保护。防止主动攻击的做法是对攻击进行检测，并从它引起的中断或延迟中恢复过来。因为检测具有威慑的效果，也可以起到预防作用。

2. 服务攻击与非服务攻击

另外，从网络高层协议的角度，攻击方法可以概括地分为两大类，即服务攻击与非服务攻击。

(1) 服务攻击(Application Dependent Attack)是针对某种特定网络服务的攻击，如针对 E-mail 服务、Telnet、FTP、HTTP 等服务的专门攻击。目前 Internet 应用协议集(主要是 TCP/IP 协议集)缺乏认证、保密措施，是造成服务攻击的重要原因。现在有很多具体的攻击工具，如 Mailf Bomb(邮件炸弹)等，可以很容易地实施对某项服务的攻击。

(2) 非服务攻击(Application Independent Attack)不针对某项具体应用服务，而是基于网络层等低层协议而进行的。TCP/IP 协议(尤其是 IPv4)自身的安全机制不足为攻击者提供了方便之门。

与服务攻击相比，非服务攻击与特定服务攻击无法相比，它往往利用协议或操作系统实现协议时的漏洞来达到攻击的目的，更为隐蔽，而且目前也是常常被忽略的方面，因而被认为是一种更为有效的且更具危险性的攻击手段。

1.3.2 基本的威胁

网络安全的基本目标是实现信息的机密性、完整性、可用性和合法性。以下 4 个基本的安全威胁直接反映了这 4 个安全目标。

(1) 信息泄露或丢失。它指敏感数据在有意或无意中被泄露出去或丢失，通常包括信息在传输中丢失或泄露、信息在存储介质中丢失或泄露、通过建立隐蔽通道等窃取敏感信息等。

(2) 破坏数据完整性。这是指以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加、修改数据，以干扰用户的正常使用。

(3) 拒绝服务攻击。它不断对网络服务系统进行干扰，改变其正常的作业流程，执行



无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

(4) 非授权访问。没有预先经过同意，就使用网络或计算机资源，被看作是非授权访问，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。它主要有假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等几种形式。

1.3.3 主要可实现的威胁

这些威胁可以使基本威胁成为可能，所以十分重要。它包括两类，即渗入威胁和植入威胁。

1. 渗入威胁的几种形式

主要的渗入威胁有：假冒、旁路控制、授权侵犯。

(1) 假冒。这是大多数黑客采用的攻击方法。某个未授权实体使守卫者相信它是一个合法的实体，从而攫取该合法用户的特权。

(2) 旁路控制。攻击者通过各种手段发现本应保密却又暴露出来的一些系统“特征”，利用这些“特征”，攻击者绕过防线守卫者渗入到系统内部。

(3) 授权侵犯。也称为“内部威胁”，授权用户将其权限用于其他未授权的目的。

2. 植入威胁的主要形式

主要的植入威胁有：特洛伊木马、后门。

(1) 特洛伊木马。攻击者在正常的软件中隐藏一段用于其他目的的程序，这段隐藏的程序段常常以安全攻击作为其最终目标。

(2) 后门。后门是在某个系统或某个文件中设置的“机关”，使得当提供特定的输入数据时允许违反安全策略。

1.3.4 病毒

病毒是能够通过修改其他程序而“感染”它们的一种程序，修改后的程序里面包含了病毒程序的一个副本，这样它们就能够继续感染其他程序。编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码被称为计算机病毒(Computer Virus)。具有破坏性、复制性和传染性。

通过网络传播计算机病毒，其破坏性大大高于单机系统，使用户很难防范。由于在网络环境下，计算机病毒有不可估量的威胁性和破坏力，因此，计算机病毒的防范是网络安全性建设的重要内容。

网络防病毒技术包括预防病毒、检测病毒和清除病毒 3 种技术。

(1) 预防病毒技术。它通过自身常驻系统内存，优先获得系统的控制权，来监视和判断系统中是否有病毒存在，进而防止计算机病毒进入计算机系统和对系统进行破坏。这类技术有加密可执行程序、引导区保护、系统监控与读写控制(如防病毒卡等)。

(2) 检测病毒技术。它是通过对计算机病毒的特征来进行判断的技术，如自身校验、

关键字、文件长度的变化等。

(3) 清除病毒技术。它通过对计算机病毒进行分析，开发出能删除病毒程序并恢复源文件的软件。

网络防病毒技术的具体实现方法包括对网络服务器中的文件进行频繁的扫描和监测；在工作站上用防病毒芯片和对网络目录及文件设置访问权限等。

1.4　影响计算机网络安全的因素

Internet 在其早期是一个开放的为研究人员服务的互联网，是非营利性的信息共享载体，所以几乎所有的 Internet 协议都没有考虑安全机制。这一点从 Internet 上最通用的应用 FTP、Telnet 和电子邮件中的用户口令的明文传输以及 IP 报文在子网段上的广播传递能充分地体现出来。但是近些年来，Internet 的性质和使用人员的情况发生了很大的变化，使得 Internet 的安全问题显得越来越突出。随着 Internet 的全球普及和商业化，用户越来越私人化，如信用卡号等同其自身利益相关的信息也通过 Internet 传输，而且越来越多的信息放在网上是为了盈利，并不是完全免费的信息共享，所以其安全性也成为人们日趋关注的问题。

1.4.1　计算机系统因素

计算机系统的脆弱性主要来自于操作系统的不安全性。在网络环境下，还来源于通信协议的不安全性。就前面所介绍的安全等级而言，全世界达到 B3 级别的操作系统只有一两个，达到 A1 级别的操作系统目前还没有。虽然 Windows XP、Windows Server 2003 和 Linux 操作系统达到了 C2 级别，但仍然存在着许多安全漏洞。

其次，每一个计算机系统都存在超级用户(如 Linux 中的 root、Windows Server 2003 中的 Administrator)，如果入侵者得到了超级用户口令，整个系统将完全受控于入侵者。现在，人们正在研究一种新型的操作系统，在这种操作系统中没有超级用户，也就不会由于有超级用户带来的问题。现在很多系统都使用静态口令来保护系统，但口令还是有很大的破解可能性，而且不完善的口令维护制度会导致口令被人盗用。口令丢失也就意味着安全系统的全面崩溃。

最后，计算机可能会因硬件或软件故障而停止运转，或被入侵者利用并造成损失。世界上没有能长久运行的计算机，计算机可能会因硬件或软件的故障而停止运转，或被入侵者利用而造成损失。硬盘故障、电源故障和芯片、主板故障都是人们应考虑的硬件故障问题，软件故障则可能出现在操作系统中，也可能出现在应用软件中。

1.4.2　操作系统因素

操作系统是计算机重要的系统软件，它控制和管理计算机所有的软、硬件资源。由于操作系统的重要地位，攻击者常常以操作系统为主要攻击目标。入侵者所做的一切，也大都是围绕着这个中心目标展开的。

首先，无论哪一种操作系统，其体系结构本身就是不安全的一种因素。由于操作系统的程序是可以动态链接的，包括 I/O 的驱动程序与系统服务都可以用打补丁的方法升级和



进行动态链接。这种方法该产品的厂商可以使用，“黑客”成员也可以利用，这种动态链接方法也正是计算机病毒产生的温床。操作系统支持的程序动态链接与数据动态交换是现代系统集成和系统扩展的必备功能，因此，这是相互矛盾的两个方面。

另一个原因在于它可以创建进程，即使在网络的节点上同样也可以进行远程进程的创建与激活，更重要的是被创建的进程具有可以继续创建进程的权力。这一点加上操作系统支持在网络上传输文件，在网络上能加载程序，二者结合起来就构成可以在远端服务器上安装“间谍”软件的条件。如果把这种“间谍”软件以打补丁的方式植入合法用户程序中，尤其是植入特权用户上，那么，系统进程与作业监视程序根本监测不到“间谍”的存在。

操作系统中，通常都有一些守护进程，这种软件实际上是一些系统进程，它们总是等待一些机会的出现。一旦有条件，程序就可以运行下去，这些软件常常被黑客利用。问题不在于有没有这些守护进程，而在于它们在 Linux、Windows 操作系统中具有与其他操作系统核心层软件同等的权限。

最后，网络操作系统提供的远程过程调用(RPC)服务以及它所安排的无口令入口也是黑客出入的通道。操作系统都提供远程进程调用(RPC)服务，而它们提供的安全验证功能却很有限。

操作系统有 Debug(调试)和 Wizard(向导)功能。许多黑客精通这些功能，利用这些技术他们几乎可以为所欲为。操作系统安排的口令入口是为系统开发人员提供的便捷入口，但也经常被黑客所利用。操作系统还提供了隐蔽的通道。这种系统不但复杂而且还存在一定的内在危险，危险之一就是授权进程或用户的访问权限可能导致用户得到限定之外的访问权力。

1.4.3　人为因素

所有的网络系统都离不开人的管理，但大多数情况下又缺少安全管理员，特别是高素质的网络管理员。人为的无意失误是造成网络不安全的重要原因。网络管理员在这方面不但肩负重任，还面临着越来越大的压力，考虑稍有不周，使安全方面配置不当，就会造成安全漏洞。另外，用户安全意识不强，不按照安全规定操作，如口令选择不慎，将自己的账户随意转借他人或与别人共享，都会对网络安全带来威胁。

1.5　计算机网络安全技术

现在，高速发展的互联网已经深入到社会生活的各个方面。对个人而言，互联网已使人们的生活方式发生了翻天覆地的变化；对企业而言，互联网改变了企业传统的营销方式及内部管理机制。但是，在享受信息的高度网络化带来的种种便利时，还必须应对随之而来的信息安全方面的种种挑战，因为没有安全保障的网络可以说是一座空中楼阁，安全性已逐渐成为网络建设的第一要素。特别是随着网络规模的逐渐增大，所存储的数据逐渐增多，使用者要想确保自己的资源不受到非法的访问与篡改，就要用到访问控制机制，这就必须要掌握一些相关的网络安全技术。

1.5.1　数据加密与认证

加密将防止数据被查看或修改，并在不安全的信道上提供安全的通信信道。加密的功能是将明文通过某种算法转换成一段无法识别的密文。在古老的加密方法中，加密的算法和加密的密钥都必须保密，否则就会被攻击者破译。例如，古人将一段羊皮条缠绕在一根圆木上，然后在其上写下要传送书信的内容，展开羊皮条后这些书信内容将变成一堆杂乱的图文，那么这种将羊皮条缠绕在圆木上的做法可视为加密算法，而圆木棍的粗细、皮条的缠绕方向就是密钥。在现代加密体系中，算法的私密性已经不再需要，信息的安全依赖于密钥的保密性。一般的数据加密模型见图 1.3。

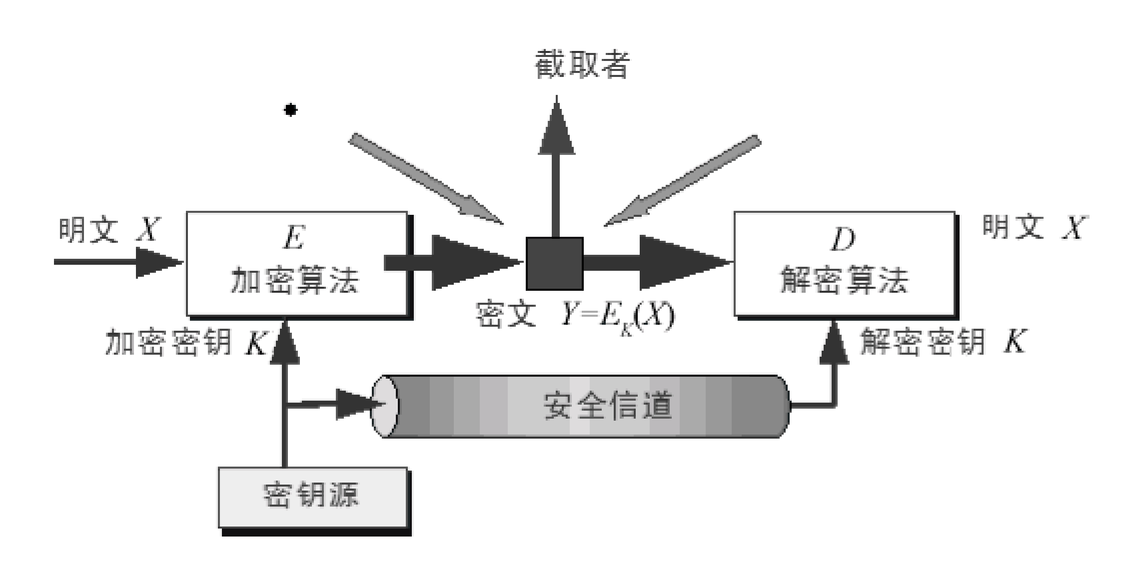


图 1.3　一般的数据加密模型

数字认证技术泛指使用现代计算机技术和网络技术进行的认证。数字认证的引入对社会的发展和进步有很大帮助，数字认证可以减少运营成本和管理费用。数字认证可以减少金融领域中的多重现金处理和现金欺诈。随着现代网络技术和计算机技术的发展，数字欺诈的现象越来越普遍，比如说，用户名下文件和资金传输可能会被伪造或更改。

数字认证提供了一种机制，使用户能证明其发出信息来源的正确性和发出信息的完整性。数字认证的另一个主要作用是操作系统可以通过它来实现对资源的访问控制。

1.5.2　防火墙

“防火墙”是一种由计算机硬件和软件的组合使互联网与内部网之间建立起一个安全网关(Security Gateway)，从而保护内部网免受非法用户的侵入。它其实就是一个把互联网与内部网(通常为局域网或城域网)隔开的屏障。

防火墙作为最早出现的网络安全产品和使用量最大的安全产品，也受到用户和研发机构的青睐。以往在没有防火墙时，局域网内部上的每个节点都暴露给 Internet 上的其他主机，此时局域网的安全性要由每个节点的坚固程度来决定，并且安全性等同于其中最弱的节点。而防火墙是放置在局域网与外部网之间的一个隔离设备，它可以识别并屏蔽非法请求，有效地防止跨越权限的数据访问。防火墙将局域网的安全性统一到它本身，网络安全性是在防火墙系统上得到加固，而不是分布在内部网络的所有节点上，这就简化了局域网的安全管理。

防火墙是由软件、硬件构成的系统，用来在两个网络之间实施接入控制策略。接入控制策略是由使用防火墙的单位自行制定的，为的是可以最适合本单位的需要。防火墙内的网络称为“可信赖的网络”(Trusted Network)，而将外部的因特网称为“不可信赖的网络”



(Untrusted Network)。防火墙可用来解决内联网和外联网的安全问题。设立防火墙的目的是保护内部网络不受外部网络的攻击，以及防止内部网络的用户向外泄密。

1.5.3　入侵检测

1. 入侵检测的概念

传统上，一般采用防火墙作为系统安全的第一道屏障。但是随着网络技术的高速发展、攻击者技术的日趋成熟以及攻击手法的日趋多样，单纯的防火墙已经不能很好地完成安全防护工作。入侵检测技术是继“防火墙”、“数据加密”等传统安全保护措施之后新一代的安全保障技术。

入侵(Intrusion)是指试图破坏计算机保密性、完整性、可用性或可控性的一系列活动。入侵活动包括非授权用户试图存取数据、处理数据或者妨碍计算机的正常运行。入侵检测(Intrusion Detection)是对入侵行为的检测，它通过收集和分析计算机网络或计算机系统中若干关键点的信息，检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。入侵检测作为一种积极、主动的安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前响应入侵并进行拦截。

2. 入侵检测的分类

1)　从技术上分类

从技术上划分，入侵检测有异常检测模型和误用检测模型两种检测模型。

(1)　异常检测模型(Anomaly Detection)：检测与可接受行为之间的偏差。如果可以定义每项可接受的行为，那么每项不可接受的行为就应该是入侵。首先总结正常操作应该具有的特征(用户轮廓)，当用户活动与正常行为有重大偏离时即被认为是入侵。这种检测模型漏报率低、误报率高。因为它不需要对每种入侵行为进行定义，所以能有效地检测未知的入侵。

(2)　误用检测模型(Misuse Detection)。检测与已知的不可接受行为之间的匹配程度。如果可以定义所有的不可接受行为，那么每种能够与之匹配的行为都会引起报警。收集非正常操作的行为特征，建立相关的特征库，当监测的用户或系统行为与库中的记录相匹配时，系统就认为这种行为是入侵。这种检测模型误报率低、漏报率高。对于已知的攻击，它可以详细、准确地报告出攻击类型，但是对未知攻击却效果有限，而且特征库必须不断更新。

2)　按照检测对象分类

按照检测对象划分，入侵检测有基于主机、基于网络和混合型 3 种模型。

(1)　基于主机。系统分析的数据是计算机操作系统的事件日志、应用程序的事件日志、系统调用、端口调用和安全审计记录。主机型入侵检测系统保护的一般是所在的主机系统，是由代理(Agent)来实现的。代理是运行在目标主机上的短小的可执行程序，它们与命令控制台(Console)通信。

(2)　基于网络。系统分析的数据是网络上的数据包。网络型入侵检测系统担负着保护整个网段的任务，基于网络的入侵检测系统由遍及网络的传感器(Sensor)组成。传感器是一台将以太网卡置于混杂模式的计算机，用于嗅探网络上的数据包。

(3) 混合型。基于网络和基于主机的入侵检测系统都有不足之处，会造成防御体系的不全面，而综合了基于网络和基于主机的混合型入侵检测系统既可以发现网络中的攻击信息，也可以从系统日志中发现异常情况。

1.5.4　计算机病毒防治

计算机病毒是一种在计算机系统运行过程中能把自身精确复制或有修改地复制到其他程序内的程序。它隐藏在计算机数据资源中，利用系统资源进行繁殖，并破坏或干扰计算机系统的正常运行。

杀毒软件是见得最多，也应用最为普遍的安全技术方案，因为这种技术实现起来最为简单，但杀毒软件的主要功能就是杀毒，功能十分有限，不能完全满足网络安全的需要。这种方式对于个人用户或小企业或许还能满足需要，但如果个人或企业有电子商务方面的需求，就不能完全满足了。可喜的是随着杀毒软件技术的不断发展，现在的主流杀毒软件同时还可以预防木马及其他的一些黑客程序的入侵。还有的杀毒软件开发商同时提供了软件防火墙，具有了一定防火墙功能，在一定程度上能起到硬件防火墙的功效，如 KV3000、金山防火墙、Norton 防火墙等。

复习思考题一

一、填空题

1. 网络安全从本质上讲就是网络上的________，是指网络系统的硬件、软件及其系统中的________受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统能连续可靠正常地运行，网络服务不中断。

2. 安全威胁是指某个人、物、事件或概念对某一资源的_______、完整性、可用性_______所造成的________。

3. 被动攻击的特点是偷听或监视传送，其目的是获得________。

4. 从技术上划分，入侵检测有两种检测模型，分别是________和________。

5. 数字认证提供了一种机制使用户能证明其发出信息来源的正确性和发出信息的完整性。数字认证的另一主要作用是_________。

6.________是一种由计算机硬件和软件的组合使互联网与内部网之间建立起一个安全网关，从而保护内部网免受非法用户的侵入。

二、单项选择题

1. 网络系统面临的威胁主要是来自人为和自然环境影响，这些威胁大致可分为 ① 两大类。入侵者对传输中的信息或存储的信息进行各种非法处理，如有选择地更改、插入、延迟、删除或复制这些信息，这是属于 ② 。入侵者通过观察网络线路上的信息，而不干扰信息的正常流动，如搭线窃听或非授权地阅读信息，这是属于 ③ 。

① (　　) A. 无意威胁和故意威胁　　B. 人为和自然环境
C. 主动攻击和被动攻击　　D. 软件系统和硬件系统

② (　　) A. 系统缺陷　　B. 漏洞威胁　　C. 主动攻击　　D. 被动攻击



③ (　　) A. 系统缺陷　B. 漏洞威胁　C. 主动攻击　D. 被动攻击

2. 计算机病毒不具有(　　)特征。

A. 破坏性　B. 隐蔽性　C. 传染性　D. 无针对性

3. 拒绝服务攻击的后果是(　　)。

A. 被攻击服务器资源耗尽　B. 被攻击者无法提供正常的网络服务

C. 被攻击者系统崩溃　D. A、B、C 都可能

三、简答题

1. 简述网络安全的基本含义。
2. 网络所面临的安全威胁主要有哪些？
3. 常用的网络安全技术有哪些？
4. 计算机病毒的定义是什么？
5. 按照检测对象划分，入侵检测有哪 3 种模型？

第 2 章　数字加密与认证技术

学习目标

系统学习密码学的基本概念，对称密钥加密和公开密钥加密技术，密钥管理的主要内容，认证机构 CA 的功能，数字签名和数字证书的功能，消息认证和身份认证的实现方法，数字证书的使用。通过本章的学习，读者应掌握以下内容:

- 掌握密码学的基本概念，数字签名和数字证书的功能，认证机构 CA 的功能，消息认证和身份认证的实现方法。
- 掌握对称密钥加密和公开密钥加密技术，密钥管理的主要内容，数字证书的使用实例。

2.1 密　码　学

数据加密是计算机网络安全很重要的一个组成部分。在因特网上进行文件传输、电子邮件商务往来存在许多不安全因素，尤其是一些机密文件在网络上传输时。而且这种不安全性是因特网本身存在的且 TCP/IP 协议所固有的，包括一些基于 TCP/IP 的服务。解决上述难题的方案就是加密，加密后的口令即使被黑客获得也是不可读的，加密后的文件没有收件人的私钥无法解开，文件成为一大堆无任何实际意义的乱码。加密在网络上的作用就是防止有用或私有化信息在网络上被拦截和窃取。文件加密不只用于电子邮件或网络上的文件传输，也可用于对静态文件的保护，如 PIP(个人信息管理)软件就可以对磁盘、硬盘中的文件或文件夹进行加密，以防他人窃取其中的信息。

加密是保障数据安全的一种方式，是一种主动的信息安全防范措施，其原理是利用加密算法，将明文转换成为无意义的密文，阻止非法用户理解原始数据，从而确保数据的保密性。明文变为密文的过程称为加密，由密文还原为明文的过程称为解密，加密和解密的规则称为密码算法。在加密和解密的过程中，由加密者和解密者使用的加、解密可变参数叫作密钥。目前，获得广泛应用的两种加密技术是对称密钥加密体制和非对称密钥加密体制。

密钥是加密运算和解密运算的关键，也是密码系统的关键。根据近代密码体制的观点，密码系统的安全取决于密钥的安全，而不是密钥算法或保密装置本身的安全。密码体制可以公开，密码设备可以丢失，同一型号的加密设备可以继续使用，但若密钥一旦丢失或出错，就会使非法用户窃取信息，将密钥泄露给他人意味着加密文档还不如使用明文，因此密钥管理在计算机的安全保密系统的设计中极为重要。密钥管理综合了密钥的产生、分配、存储、组织、使用、销毁等一系列技术问题，同时又包含了行政管理和人员素质问题。

为保证网络信息的安全，当今世界各主要国家的政府部门都十分重视密码工作，有的设立庞大机构，拨出巨额经费，集中数以万计的专家和科技人员，投入大量高速的电子计算机和其他先进设备进行研究。同时，企业界和学术界也对密码设置日益重视，不少数学家、计算机学家和其他有关学科的专家也投身于密码学的研究行列，这些都加快了密码学



的发展。

2.1.1 加密的起源

加密作为保障数据安全的一种方式，其起源要追溯到公元前 2000 年，埃及人是最先使用象形文字作为信息编码的，随着时间的推移，巴比伦、美索不达米亚和希腊文明都开始使用一些方法来保护它们的书面信息。

近期加密技术主要应用于军事领域，最广为人知的编码机器是 German Enigma 机。在第二次世界大战中，德国人利用它创建了加密信息。当初，计算机的研究就是为了破解德国人的密码，人们并没有想到计算机为今天带来的信息革命。随着计算机运算能力的增强，过去的加密就变得十分简单，于是人们又不断地研究出新的数据加密方式，如利用 RSA 算法产生的私钥和公钥就是在这个基础上应运而生的。

2.1.2 密码学基本概念

密码学是研究编制密码和破译密码的技术科学。研究密码变化的客观规律，应用于编制密码以保守通信秘密的，称为编码学；应用于破译密码以获取通信情报的，称为破译学，统称密码学。

密码是通信双方按约定的规则进行信息交流的一种重要保密手段。依照这些法则，变明文为密文，称为加密变换；变密文为明文，称为解密变换。早期密码仅对文字或数码进行加、解密变换，随着通信技术的发展，对语音、图像、数据等都可实施加、解密变换。

加密有载体加密和通信加密两种。密码学主要研究通信加密，而且仅限于数据通信加密。

要详细、深入地了解密码学，首先要掌握以下基本术语。

- 密码(Cipher)。用来检查对系统或数据未经验证访问的安全性的术语或短语。
- 加密(Encipher)。通过密码系统把明文变换为不可懂的形式的密文。
- 加密算法(Encryption Algorithm)。实施一系列变换，使信息变成密文的一组数学规则。
- 解密(Decrypt)。使用适当的密钥，将已加密的文本转换成明文。
- 密文(Ciphertext)。经过加密处理而产生的数据，其语义内容是不可用的。
- 明文(Plaintext)。可理解的数据，其语义内容是可用的。
- 公共密钥。公共密钥是加密系统的公开部分，只有所有者才知道私用部分的内容。
- 私有密钥。公钥加密系统的私有部分。私有密钥是保密的，不通过网络传输。
- 数字签名(Signature)。附加在数据单元上的一些数据，或是对数据单元所作的密码变换。这种数据或变换允许数据单元的接收者用以确认数据单元的来源和数据单元的完整性，并保护数据，防止被他人(如接收者)伪造。
- 身份认证(Authentication)。验证用户、设备和其他实体的身份；验证数据的完整性。
- 机密性(Confidentiality)。这一性质使信息不泄露给非授权的个人、实体或进程，不为其所用。
- 数据完整性(Data Integrity)。信息系统中的数据与原文档相同，未曾遭受偶然或恶

意的修改或破坏。

- 防抵赖(Non-Repudiation)。防止在通信中涉及的实体不承认参加了该通信的全部或一部分。

其中加密与解密是一对相反的概念，图 2.1 给出了加密与解密过程的示意图。

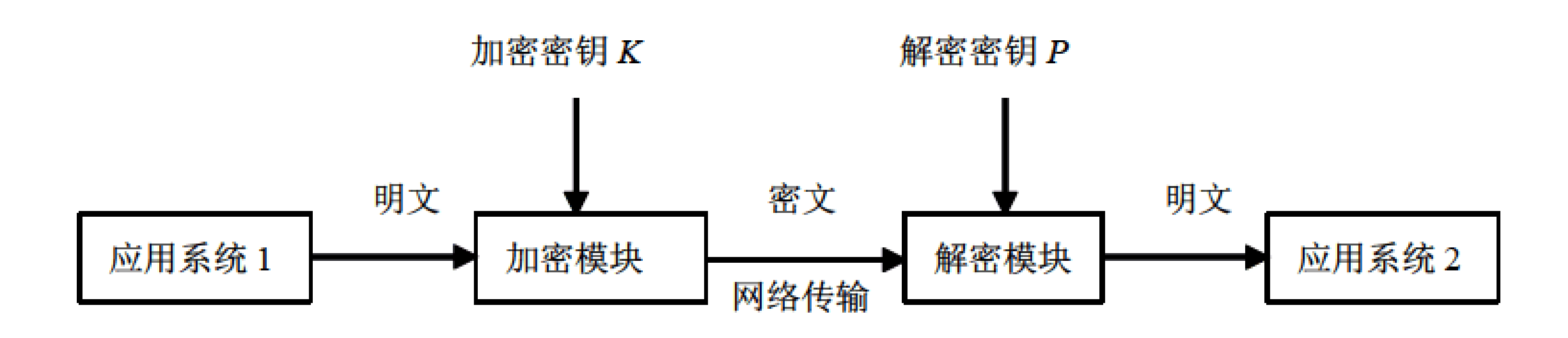


图 2.1　加密与解密过程示意图

2.1.3　传统加密技术

传统的加密方法可以分为替代密码与换位密码两类。

1. 替代密码

在替代密码中，用一组密文字母来代替一组明文字母可以隐藏明文，但保持明文字母位置不变。

最古老的替代密码是恺撒密码，它用 D 表示 a，用 E 表示 b，用 F 表示 c，……，用 C 表示 z，也就是说密文字母相对明文字母左移了 3 位。为清楚起见，一律用小写表示明文，用大写表示密文，这样明文的“cipher”就变成了密文的“FLSKHU”。更一般地，可以让密文字母相对明文字母左移 *K* 位，这样 *K* 就成了加密和解密的密钥。这种密码是很容易破译的，因为最多只需尝试 25 次(*K*=1～25)即可轻松破译密码。

较为复杂的密码使明文字母和密文字母之间互相映射，它没有规律可循，比如将 26 个英文字母随意映射到其他字母上，这种方法称为单字母表替换，其密钥是对应于整个字母表的 26 个字母。虽然初看起来这个系统是很安全的，因为若要试遍所有 26 种可能的密钥，即使计算机每微秒试一个密钥，也需要 1013 年。但事实上完全不需要这么做，破译者只要拥有很少一点密文，利用自然语言的统计特征，很容易就可破译密码。破译的关键在于找出各种字母或字母组合出现的频率，比如经统计发现，英文中字母 e 出现的频率最高，其次是 t、o、a、n、i 等，最常见的两字母组合依次为 th、in、er、re 和 an，最常见的 3 字母组合依次为 the、ing、and 和 ion。因此破译者首先可将密文中出现频率最高的字母定为 e，频率次高的字母定为 t，然后猜测最常见的两字母组、3 字母组，比如密文中经常出现 tXe，就可以推测 X 很可能就是 h，如经常出现 thYt，则 Y 很可能就是 a 等。采用这种合理的推测，破译者就可以逐字逐句组织出一个试验性的明文。

为去除密文中字母出现的频率特征，可以使用多张密码字母表，对明文中不同位置上的字母用不同的密码字母表来加密。比如任意选择 26 张不同的单字母密码表，相互间排定一个顺序，然后选择一个简短易记的单词或短语作为密钥，在加密一条明文时，将密钥重复写在明文的上面，则每个明文字母上的密钥字母即指出该明文字母用哪一张单字母密码表来加密。

比如要加密明文“please carry the last plan”，密钥为“computer”，则将“computer”重复写在报文上面，如图 2.2 所示。



c	o	m	p	u	t	e	r	c	o	…	c	o	m	p	u	t	e	r	c
p	l	e	a	s	e	c	a	r	r	…	e	l	a	s	t	p	l	a	n

图 2.2　把一段明文用密钥为“computer”进行加密

于是第 1 个明文字母 p 用第 3 张(假设 a～z 分别表示顺序 1～26)单字母密码表加密，第 2 个明文字母 l 用第 12 张单字母密码表加密……显然，同一个明文字母因位置不同而在密文中可能用不同的字母来表示，从而消除了各种字母出现的频率特征。

虽然破译多字母密码表要困难一些，但如果破译者手头有较多的密文，仍然是可以破译的，破译的诀窍在于猜测密钥的长度。首先破译者假设密钥的长度，然后将密文按每行 k 个字母排成若干行，如果猜测正确，那么同一列的密文字母应是用同一单字母密码表加密的，因此同一列中各密文字母的频率分布应与英文相同，即最常用的字母(对应明文字母 e)频率为 13%，次常用的字母(对应明文字母 t)频率为 9%等。如果猜测不正确，则换一个 k 值重试，一旦猜测正确，即可逐列使用破译单字母表密码的方法进行破译。

2. 换位密码

换位密码(又叫置换加密)是将明文字母互相换位，明文的字母保持相同，但顺序被打乱。它最大的特点是不需对明文字母作任何变换，只需对明文字母的顺序按密钥的规律相应地排列组合后输出形成密文。

线路加密法是一种换位加密。在线路加密法中，明文的字母按规定的次序排列在矩阵中，然后用另一种次序选出矩阵中的字母，排列成密文。如纵行换位密码中，明文以固定的宽度水平地写出，密文按垂直方向读出。

明文：COMPUTERGRAPHICSMAYBESLOWBUTATLEASTITSEXPENSIVE

将明文按长度 10 为一行，排成纵列：

COMPUTERGR
APHICSMAYB
ESLOWBUTAT
LEASTITSEX
PENSIVE

然后按垂直方向写出密文：

密文：CAELPOPSEEMHLANPIOSSUCWTITSBIVEMUTERATSGYAERBTX

从上例可以看出，无论怎样换位置，密文字符与明文字符的数目保持相同，对密文字母的统计分析很容易决定字母的准确顺序。

此种加密方法保密程度较高，但其最大的缺点是密文呈现字母自然出现频率，破译者只要稍加统计即可识别此类加密方法，然后采取先假定密钥长度的方法，对密文进行排列组合，借助计算机的高速运算能力及常用字母的组合规律，也可以进行不同程度的破译。

以上是传统加密的方法，它有以下特点：其一是加密密钥与解密密钥相同；其二是加密算法比较简单，主要侧重于增加密钥长度以提高保密程度。



2.1.4　对称密钥算法

现代密码学也使用替代密码和换位密码的思想，但和传统密码学的侧重点不同，传统密码学的加密算法比较简单，主要通过增加密钥长度来提高保密程度；而现代密码学正好相反，它使用极为复杂的加密算法，即使破译者能够对任意数量的选择明文进行加密，也无法找出破译密文的方法。

对称算法就是加密密钥能够从解密密钥中推算出来，反过来也成立。在大多数对称算法中，加、解密密钥是相同的。这些算法也叫秘密密钥算法或单密钥算法。

1. 对称密钥算法加密的要求

(1)　需要强大的加密算法。即使对手知道了算法并能访问一些或更多的密文，也不能破译密文或得出密钥。

(2)　发送方和接收方必须用安全的方式来获得保密密钥的副本，必须保证密钥的安全。如果有人发现了密钥，并知道了算法，则使用此密钥的所有通信便都是可读取的。

常规机密的安全性取决于密钥的保密性，而不是算法的保密性。也就是说，如果知道了密文和加密及解密算法的知识，解密消息也是不可能的。

2. 一些常用的对称密钥加密算法

(1)　数据加密标准(DES)。

最常用的加密方案是美国国家标准和技术局(NIST)在 1977 年采用的数据加密标准(Data Encryption Standard，DES)，它是联邦信息处理第 46 号标准(FIPS PUB 46)。DES 主要采用替换和移位的方法加密，它用 56 位密钥对 64 位二进制数据块进行加密，每次加密可对 64 位数据进行 16 轮编码，经一系列替换和移位后，输入的 64 位原始数据转换成完全不同的 64 位输出数据。

DES 算法适用于最大为 64 位的标准算术和逻辑运算，运算速度快，密钥产生容易，适合于在当前大多数计算机上用软件方法实现，同时也能在专用芯片上实现。DES 算法的弱点是不能提供足够的安全性，因为其密钥容量只有 56 位。由于这个原因，后来又提出了 3 重 DES 系统，使用 3 个不同的密钥对数据块进行(两次或)3 次加密，该方法比进行普通加密的 3 次快。其强度大约和 112bit 的密钥强度相当。算法本身以数据加密算法(Data Encryption Algorithm，DEA)被引用。DES 本身虽已不再安全，但其改进算法的安全性还是相当可靠的。

(2)　国际数据加密算法(IDEA)。

数据加密算法(Internation Data Encryption Algorithm，IDEA)是由瑞士的两位科学家于 1990 年联合提出的，它的明文和密文都是 64bit，但密钥长为 128bit。IDEA 是作为迭代的分组密码实现的，使用 128 位的密钥和 8 个循环。这比 DES 提供了更多的安全性，但是在选择用于 IDEA 的密钥时，应该排除那些称为“弱密钥”的密钥。DES 只有 4 个弱密钥和 12 个次弱密钥，而 IDEA 中的弱密钥数相当可观，有 2^{51} 个。但是，如果密钥的总数非常大，达到 2^{128} 个，那么仍有 2^{77} 个密钥可供选择。IDEA 被认为是极为安全的。使用 128 位的密钥，暴力攻击中需要进行的测试次数与 DES 相比会明显增大，甚至允许对弱密钥测试。



解密密钥必须和加密密钥相同，这是对称密钥算法的一个弱点，这就产生了如何安全地分发密钥的问题。传统上是由一个中心密钥生成设备产生一个相同的密钥对，并由人工信使将其传送到各自的目的地。对于一个拥有许多部门的组织来说，这种分发方式是不能令人满意的，尤其是出于安全方面的考虑需要经常更换密钥时更是如此。此外，两个完全陌生的人要想秘密通信，就必须通过实际会面来商定密钥，否则别无他法。1976 年，Diffie 和 Hellman 提出了一种全新的加密思想——公开密钥算法，很好地解决了这个问题。

2.1.5　公开密钥算法

公开密钥加密最初是由 Diffie 和 Hellman 在 1976 年提出的，这是几千年来文字加密的第一次真正革命性的进步。公钥是建立在数学函数基础上，而不是建立在位方式的操作上。更重要的是，公钥加密是不对称的，与只使用一种密钥的对称常规加密相比，它涉及公钥和私钥的使用。这两种密钥的使用已经对机密性、密钥的分发和身份验证领域产生了深远的影响。公钥加密算法可用于数据完整性、数据保密性、发送者不可否认和发送者认证等方面。

在公开密钥算法提出之前，所有密码系统的解密密钥和加密密钥都有很直接的联系，即从加密密钥可以很容易地导出解密密钥，因此所有的密码学家理所当然地认为应对加密密钥进行保密。但是 Diffie 和 Hellman 提出了一种完全不同的设想，从根本上改变了人们研究密码系统的方式。

在 Diffie 和 Hellman 提出的方法中，加密密钥和解密密钥是不同的，并且从加密密钥不能得到解密密钥。为此，加密算法 E 和解密算法 D 必须满足以下 3 个条件：

(1)　$D(E(P))=P$。

(2)　从 E 导出 D 非常困难。

(3)　由一段明文不可能破译出 E。

第①个条件是指将解密算法 D 作用于密文 $E(P)$后就可获得明文 P；第②个条件是不可能从 E 导出 D；第③个条件是指破译者即使能加密任意一段明文，也无法破译密码。如果能够满足以上 3 个条件，则加密算法完全可以公开。

Diffie 和 Hellman 算法的基本思想是：如果某个用户希望接收秘密报文，他必须设计两个算法，即加密算法 E 和解密算法 D，然后将加密算法放于任何一个公开的文件中广而告之，这也是公开密钥算法名称的由来，他甚至还可以公开他的解密方法，只要妥善保存解密密钥即可。当两个完全陌生的用户 A 和 B 希望进行秘密通信时，各自可以从公开的文件中查到对方的加密算法；若 A 需要将秘密报文发给 B，则 A 用 B 的加密算法 E_B 对报文进行加密，然后将密文发给 B，B 使用解密算法 D_B 进行解密，而除 B 以外的任何人都无法读懂这个报文；当 B 需要向人发送消息时，B 使用 A 的加密算法 E_A 对报文进行加密，然后发给 A，A 利用 D_A 进行解密。

在这种算法中，每个用户都使用两个密钥，其中加密密钥是供其他人发送报文用的，是公开的；解密密钥是用于对收到的密文进行解密的，是保密的。通常用公开密钥和私人密钥分别称呼公开密钥算法中的加密密钥和解密密钥，以同传统密码学中的秘密密钥相区分。由于私人密钥只由用户自己掌握，不需要分发给别人，也就不用担心在传输的过程中或被其他用户泄密，因而是极其安全的。用公开密钥算法解决上面所说的密钥分发问题非

常简单，中心密钥生成设备产生一个密钥后，用各个用户公开的加密算法对之进行加密，然后分发给各用户，各用户再用自己的私人密钥进行解密，操作既安全又省事。两个完全陌生的用户之间也可以使用这种方法方便地商定一个秘密的会话密钥。

由于公开密钥算法潜在的优越性，研究者们一直在努力寻找符合以上 3 个条件的算法，已经有一些算法被提了出来，其中较好的一个是由 MIT 的一个研究小组提出的，并以 3 个发现者名字的首字母命名，称为 RSA 算法。RSA 算法基于一些数论的原理，在此不对它做理论上的推导，只说明如何使用这种算法。

- 选择两个大素数 p 和 q(典型值为大于 10100)。
- 计算 $n=p\times q$ 和 $z=(p-1)(q-1)$。
- 选择一个与 z 互质的数，令其为 d。
- 找到一个 e 使满足 $ed=1 \bmod z$。

计算以上参数后，就可以对明文加密。首先将明文看成是一个位串，将其划分成一个个的数据块 P 且 $0\leqslant P<n$。要做到这一点并不难，只需先求出满足 $2k<n$ 的最大 k 值，然后使得每个数据块长度不超过 k 即可。对数据块 P 进行加密，计算 $C=P^e(\bmod\ n)$，C 即为 P 的密文；对 C 进行解密，计算 $P=C^d(\bmod\ n)$。可以证明，对于指定范围内的所有 P 其加密函数和解密函数互为反函数。进行加密需要参数 e 和 n，进行解密需要参数 d 和 n，所以公开密钥由(e，n)组成，私人密钥由(d，n)组成。

RSA 算法的安全性建立在难以对大数提取因子的基础上，如果破译者能对已知的 n 提取出因子 p 和 q 就能求出 z，知道了 z 和 e，就能利用 Euclid 算法求出 d。所幸的是，300 多年来虽然数学家们已对大数因式分解的问题做了大量研究，但并没有取得任何进展，到目前为止这仍是一个极其困难的问题。据 Rivest 等的推算，用最好的算法和指令时间为 1μs 的计算机对一个 200 位的十进制数作因式分解需要 40 亿年的机器时间，而对一个 500 位的数作因式分解需要 1025 年。即使计算机的速度每 10 年提高一个数量级，能作 500 位数的因式分解也是在若干世纪之后，然而到那时，人们只要选取更大的 p 值和 g 值就行了。

为了演示 RSA 算法的使用，在此举一个简单的例子。假设取 $p=3$，$q=11$，则计算出 $n=33$ 和 $z=20$。由于 7 和 20 没有公因子，因此可取 $d=7$；解方程 $7e=1(\bmod\ 20)$可以得到 $e=3$。由此公开密钥为(3，33)，私人密钥为(7，33)。假设要加密的明文为 $M=4$，则 $C=M^e(\bmod\ n)=4^3(\bmod\ 33)=31$，于是对应的密文为 $C=31$。接收方收到密文后进行解密，计算 $M=C^d(\bmod\ n)=31^7(\bmod\ 33)=4$，恢复出原文。

应该指出的是，与对称密码体制如 DES 相比，虽然 RSA 算法具有安全、方便的特点，但它的运行速度太慢，因此，RSA 体制很少用于数据加密，而多用在数字签名、密钥管理和认证等方面，数据的加密仍使用秘密密钥算法。

1985 年，Elgamal 构造了一种基于离散对数的公钥密码体制，这就是 Elgamal 公钥体制。Elgamal 公钥体制的密文不仅依赖于待加密的明文，而且依赖于用户选择的随机参数，即使加密相同的明文，得到的密文也是不同的。由于这种加密算法的非确实性，又称其为概率加密体制。在确定性加密算法中，如果破译者对某些关键信息感兴趣，则他可事先将这些信息加密后存储起来，一旦以后截获密文，就可以直接在存储的密文中进行查找，从而求得相应的明文。概率加密体制弥补了这种不足，进一步提高了安全性。

与既能作公钥加密又能作数字签名的 RSA 不同，Elgamal 签名体制是在 1985 年仅为数



字签名而构造的签名体制。NIST 采用修改后的 Elgamal 签名体制作为数字签名体制标准。破译 Elgamal 签名体制等价于求解离散对数问题。

背包公钥体制是 1978 年由 Merkle 和 Hellman 提出的。背包算法的思路是假定某人拥有大量的物品，重量各不相同。此人通过秘密地选择一部分物品并将它们放到背包中来加密消息。背包中的物品总重量是公开的，所有可能的物品也是公开的，但背包中的物品却是保密的。附加一定的限制条件，给出重量，而要列出可能的物品，在计算上是不可实现的。这就是公开密钥算法的基本思想。

大多数公钥密码体制都会涉及高次幂运算，不仅加密速度慢，而且会占用大量的存储空间。背包问题是熟知的不可计算问题，背包体制以其加密、解密速度快而引人注目。但是，大多数一次背包体制均被破译了，因此很少有人使用它。

目前许多商业产品采用的公钥算法还有 Diffie-Hellman 密钥交换、数据签名标准 DSS 和椭圆曲线密码技术等。

2.1.6　加密技术在网络中的应用

加密技术用于网络安全通常有两种形式，即面向网络服务或面向应用服务。

面向网络服务的加密技术工作在网络层或传输层，使用经过加密的数据包传送、认证网络路由以及其他网络协议所需的信息，从而保证网络的连通性和可用性不受损害。在网络层上实现的加密技术对于网络应用层的用户而言是透明的。此外，通过适当的密钥管理机制，使用这一方法还可以在公用网络上建立虚拟专用网络，并保障其信息安全性。

面向网络应用服务的加密技术是目前较为流行的加密技术，如使用 Kerberos 服务的 Telnet、NFS、Rlogin 等，以及用作电子邮件加密的 PEM(Privacy Enhanced Mail)和 PGP(Pretty Good Privacy)。这一类加密技术实现起来相对较为简单，不需要对电子信息(数据包)所经过的网络安全性能提出特殊要求，对电子邮件数据实现端到端的安全保障。

从通信网络的传输方面，数据加密技术还可分为以下 3 类，即链路加密方式、节点到节点方式和端到端方式。

(1) 链路加密方式是普通网络通信安全主要采用的方式。它不但对数据报文的正文进行加密，而且把路由信息、校验码等控制信息全部加密。所以，当数据报文到某个中间节点时，必须被解密以获得路由信息和校验码，进行路由选择、差错检测，然后才能被加密，发送到下一个节点，直到数据报文到达目的节点为止。

(2) 节点到节点加密方式是为了解决在节点中数据明文传输的缺点，在中间节点里装有加、解密的保护装置，由这个装置来完成一个密钥向另一个密钥的交换。因而，除了在保护装置内，即使在节点内也不会出现明文。但是这种方式和链路加密方式一样需要公共网络提供者配合，修改它们的交换节点，增加安全单元或保护装置。

(3) 在端到端加密方式中，由发送方加密的数据在没有到达最终目的节点之前是不被解破的，加、解密只在源、宿节点进行，因此，这种方式可以按各种通信对象的要求改变加密密钥，以及按应用程序进行密钥管理等，而且采用这种方式可以解决文件加密问题。

链路加密方式和端到端加密方式的区别是，链路加密方式是对整个链路的通信采用保护措施，而端到端方式则是对整个网络系统采取保护措施。因此，端到端加密方式是未来的发展趋势。



2.1.7 密码分析

试图发现明文或密钥的过程称为密码分析。密码分析人员使用的策略取决于加密方案的特性和分析人员可用的信息。密码分析的过程通常包括分析(统计所截获的消息材料)、假设、推断和证实等步骤。

表 2.1 总结了各类加密消息的破译类型，这些破译是以分析人员所知的信息总量为基础的。在一些情况下，分析人员可能根本就不知道加密算法，但一般可以认为已经知道了加密算法。这种情况下，最可能的破译就是用暴力攻击(或称为穷举攻击)来尝试各种可能的密钥。如果密钥空间很大，这种方法就行不通了。因此，必须依赖于对密文本身的分析，通常会对它使用各种统计测试。

表 2.1 加密消息的破译类型

破译类型	密码分析人员已得到的内容
仅密文	加密算法、要解密的密文
已知明文	加密算法、要解密的密文、使用保密密钥生成的一个或多个明文-密文对
选择明文	加密算法、要解密的密文、密码分析人员选择的明文消息，以及使用保密密钥生成的对应的密文对
选择密文	加密算法、要解密的密文、密码分析人员选择的密文，以及使用保密密钥生成的对应的解密明文
选择文本	加密算法、要解密的密文、密码分析人员选择的明文消息，以及使用保密密钥生成的对应的密文对、密码分析人员选择的密文，以及使用保密密钥生成的对应的解密明文

只针对密文的破译是比较困难的，因为可用信息量很少。但是，在很多情况下，分析者能够捕获一些或更多的明文信息及其密文，或者分析者已经知道信息中明文信息出现的格式。例如，PostScript 格式中的文件总是以同样的方式开始，或者电子资金的转账存在着标准化的报头或标题等。这些都是已知明文的示例，有了这些知识，分析者就能够在已知明文传送方式的基础上推导出密钥。

与已知明文的攻击方式密切相关的是词语攻击方式。如果分析者面对的是一般平铺直叙的加密消息，则他几乎就不能知道消息的内容是什么。但是，如果分析者拥有一些非常特殊的信息，就有可能知道消息中其他部分的内容。

2.2 密 钥 管 理

密钥管理是数据加密技术中的重要一环，密钥管理的根本意图在于提高系统的安全保密程度。一个良好的密钥管理系统，除在生成与分发过程中尽量减少人力直接干预外，还应做到以下几点：

(1) 密钥难以被非法窃取。

(2) 在一定条件下，即使被窃取了也无用。

(3) 密钥分发和更换的过程，对用户是透明的，用户不一定亲自掌握密钥。



密钥是加密运算和解密运算的关键，也是密码系统的关键。密码系统的安全取决于密钥的安全，而不是密钥算法或保密装置本身的安全。即使公开了密码体制，或者丢失了密码设备，同一型号的加密设备也仍然可以继续使用；但若密钥一旦丢失或出错，就会被非法用户窃取信息。将密钥泄露给他人意味着加密文档还不如使用明文，因此密钥管理在计算机的安全保密系统的设计中极为重要。密钥管理综合了密钥的产生、分发、存储、组织、使用、销毁等一系列技术问题，同时也对行政管理和人员素质提出了要求。

2.2.1 密钥的分类和作用

在同一密码系统中，为保证信息和系统安全，常常需要多种密钥，每种密钥担负相应的任务。下面介绍几种常用的密钥。

(1) 初级密钥。把保护数据(加密和解密)的密钥叫作初级密钥(K)，初级密钥又叫数据加密(数据解密)密钥。当初级密钥直接用于提供通信安全时，叫作初级通信密钥(KC)。在通信会话期间用于保护数据的初级通信密钥叫作会话密钥，但初级密钥用于直接提供文件安全时，叫作初级文件密钥(KF)。

(2) 钥加密钥。对密钥进行保护的密钥称为钥加密钥，把保护初级密钥的密钥叫作二级密钥(KN)，同样可以分为二级通信密钥(KNC)和二级文件密钥(KNF)。

(3) 主机密钥。一个大型的网络系统可能有上千个节点或端用户，若要实现全网互通，每个节点就要保存用于与其他节点或端用户进行通信的二级密钥和初级密钥，这些密钥要形成一张表保存在节点(或端节点的保密装置)内，若以明文的形式保存，有可能会被窃取。为保证它的安全，通常还需要有一个密钥对密钥表进行加密保护，此密钥称为主机密钥或主控密钥。

(4) 其他密钥。在一个系统中，除了上述密钥外，还可能有通播密钥、共享密钥等，它们也有各自的用途。

2.2.2 密钥长度

密钥长度一般是以二进制位(bit)为单位，也有以字节(Byte)为单位的，密钥的长度对密钥的强度有直接的影响。密钥的长度涉及两个问题：多长的密钥才适合保密通信的要求；密钥系统对于对称/非对称密钥长度的匹配问题。

1. 密钥长度的要求

密钥长度的要求与信息安全需要的环境有关，表 2.2 列出了不同信息安全需要对于对称/非对称密钥尺度的要求。

表 2.2 不同信息安全需要对密钥尺度的要求

信息类型	时　间	对称密钥的长度(bit)	公开密钥的长度(bit)
战场军事信息	数分钟/小时	56～64	384
产品发布、合并、利率	几天/小时	64	512

续表

信息类型	时 间	对称密钥的长度(bit)	公开密钥的长度(bit)
长期商业计划	几年	112	1792
贸易秘密	几十年	128	2304
氢弹秘密	>40 年	128	2304
间谍身份	>50 年	128	2304
个人隐私	>50 年	128	2304
外交秘密	>65 年	至少 128	至少 2304

表 2.2 表明了安全环境对密钥长度的制约。由于计算机技术和密码学的发展，密钥长度已经有了很大的变化，比如对称密钥的长度已经修改为 128～192bit。

2. 对称/非对称密钥长度的匹配

无论是使用对称密钥算法还是公开密钥算法，其设计的系统都应该对密钥长度有具体的要求，以防止穷举等攻击的破译。穷举攻击是指用所有可能的密钥空间中的密钥值破译加密信息。因此，表 2.2 表明，如果同时使用 64bit 的对称密钥算法和 384bit 的公开密钥算法是没有什么安全可言的，如果希望使用的对称算法的密钥长度是 128bit，那么使用的公开算法的密钥长度至少应为 2304 位。

如果使用更长一些的密钥，就必须为密钥变长所需计算时间付出代价。通常，使密钥足够长，而计算所需的时间足够短。表 2.3 给出了公开密钥多长才安全的一些忠告。其中，每年度列出了 3 个密钥长度，分别针对个人、大公司和政府。

表 2.3 公开密钥长度的推荐值(bit)

年 度	对于个人	对于大公司	对于政府
1995	768	1280	1536
2000	1024	1280	1536
2005	1280	1536	2048
2010	1280	1536	2048
2015	1536	2048	2048

诚然，对称密钥和公开密钥就密钥长度的比较而言，使用对称密钥的算法在实现上比公开密钥的算法要快很多，而且密钥长度也要短。但是，公钥技术具有更大的实际使用效果。一般而言，应该选择比对称密钥算法更安全的公开密钥长度，因为公开密钥算法通常持续时间长，而且可保护更多的信息。

2.2.3 密钥的产生技术

1. 密钥的随机性要求

密钥是数据保密的关键，应有足够的方法来产生密钥。作为密钥的一个基本要求是要具有良好的随机性。



在普通的非密码应用场合，人们只要求所产生出来的随机数呈现平衡的、等概率的分布，而不要求它的不可预测性。而在密码技术中，特别是在密钥产生技术中，不可预测性成为随机性的一个最基本要求，因为那些虽然能经受随机统计检验但很容易预测的序列肯定是容易被攻破的。

2. 产生密钥的方法

现代通信技术中需要产生大量的密钥，以分配给系统中的各个节点和实体，如果产生密钥的方式很难适应大量密钥需求的现状，因此实现密钥产生的自动化，不仅可以减轻人工产生密钥的工作负担，还可以消除人为因素引起的泄密。

1) 密钥产生的硬件技术

噪声源技术是密钥产生的常用方法，因为噪声源的功能就是产生二进制的随机序列或与之对应的随机数，它是密钥产生设备的核心部件。噪声源的另一个功能是在物理层加密的环境下进行信息填充，使网络能够防止流量分析。噪声源技术还被用于某些身份验证技术中。例如，在对等实体中，为防止口令被窃取常常使用随机应答技术，这时的提问与应答都是由噪声控制的。

如果噪声源的随机性不强，就会给破译带来线索，某些破译方法还特别依赖于加密者使用简单的或容易猜破的密钥。

噪声源输出的随机数序列按照产生的方法可以分为以下几种：

(1) 伪随机序列。伪随机序列也称作伪码，具有近似随机序列(噪声)的性质，而又能按照一定规律(周期)产生和复制的序列。因为真正的随机序列是只能产生而不能复制的，所以称其“伪”随机序列。通常用数学方法和少量的种子密钥来产生。伪随机序列一般都有良好的、能经受理论检验的随机统计特性。常用的伪随机序列有 *m* 序列、*M* 序列和 R-S 序列。

(2) 物理随机序列。它指用热噪声等方法产生的随机序列。实际的物理噪声往往要受到温度、电源、电路特性等因素的制约，其统计特性常常带有一定的偏向性。

(3) 准随机序列。用数学方法和物理方法相结合产生的随机序列，它可以克服两者的缺点。

2) 密钥产生的软件技术

X9.17(X9.17-1985 金融机构密钥管理标准，由 ANSI－美国国家标准定义)标准定义了一种产生密钥的方法，如图 2.3 所示。

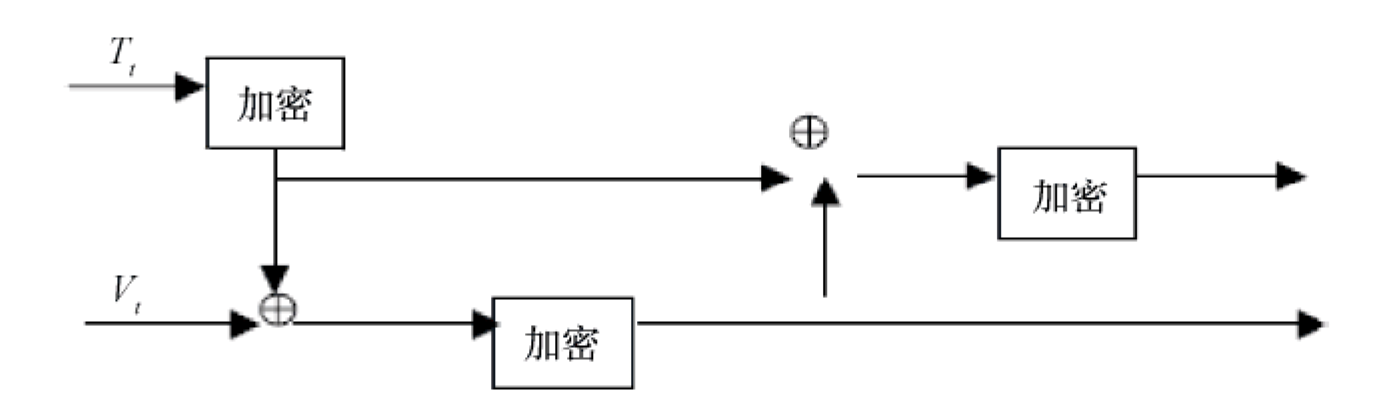


图 2.3　ANSI X9.17 密钥产生的过程

X9.17 标准产生密钥的算法是 3 重 DES，算法的目的并不是产生容易记忆的密钥，而是在系统中产生一个会话密钥或是伪随机数。其过程如下：

假设 $E_k(x)$表示用密钥 K 对比特串 x 进行的三重 DES 加密，K 是为密钥发生器保留的一个特殊密钥。V_0 是一个秘密的 64 位种子，T 是一个时间标记。欲产生的随机密钥 R_i 可以通过下面的两个算式来计算：

$$R_i = E_k(E_k(T_i) \oplus V_i)$$

$$V_i = E_k(E_k(T_i) \oplus R_i)$$

对于 128bit 或 192bit 密钥，可以通过以上方法生成几个 64bit 的密钥后，串接起来便可。

3)　针对不同密钥类型的产生方法

(1)　主机主密钥的产生。这类密钥通常要用诸如掷硬币、骰子、从随机数表中选数等随机方式产生，以保证密钥的随机性，避免可预测性。而任何机器和算法所产生的密钥都有被预测的危险，主机主密钥是控制产生其他加密密钥的密钥，而且长时间保持不变，因此它的安全性是至关重要的。

(2)　加密密钥的产生。加密密钥可以由机器自动产生，也可以由密钥操作员选定。加密密钥构成的密钥表存储在主机中的辅助存储器中，只有密钥产生器才能对此表进行增加、修改、删除和更换密钥，其副本则以秘密方式送给相应的终端或主机。一个有 n 个终端用户的通信网，若要求任一对用户之间彼此能进行保密通信，则需要 $n(n-1)/2$ 个密钥加密密钥。当 n 较大时，难免有一个或数个被敌手掌握。因此密钥产生算法应当能够保证其他用户的密钥加密密钥仍有足够的安全性。可用随机比特产生器(如噪声二极管振荡器等)或伪随机数产生器生成这类密钥，也可用主密钥控制下的某种算法来产生。

(3)　会话密钥的产生。会话密钥可在密钥加密密钥作用下通过某种加密算法动态地产生，如用初始密钥控制一非线性移位寄存器或用密钥加密密钥控制 DES 算法产生。初始密钥可用产生密钥加密密钥或主机主密钥的方法生成。

2.2.4　密钥的组织结构

一个密钥系统可能有若干种不同的组成部分，按照它们之间的控制关系，可以将各个部分划分为一级密钥、二级密钥、……、n 级密钥，组成一个 n 级密钥系统，如图 2.4 所示。

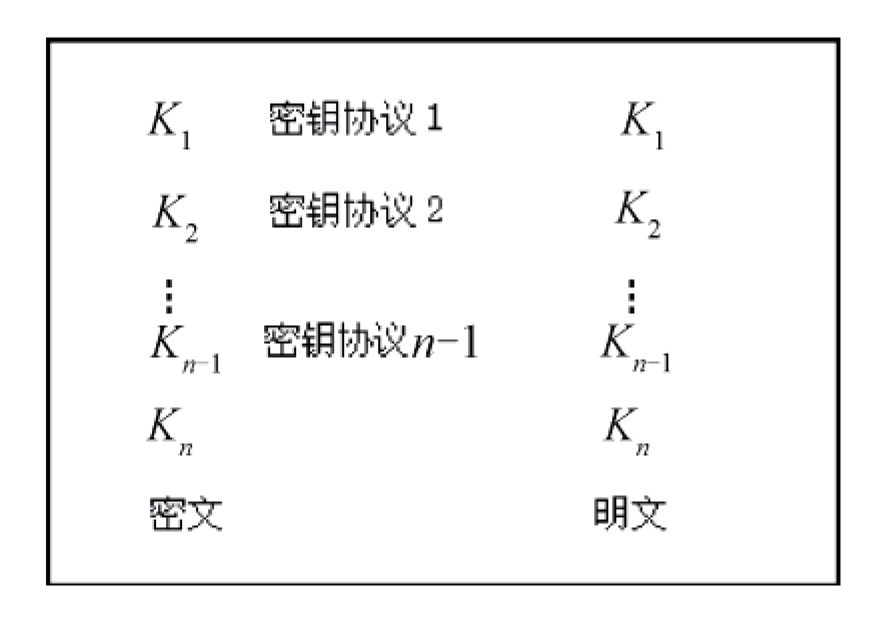


图 2.4　多层密钥系统机构示意图

其中，一级密钥用算法 f_1 保护二级密钥，二级密钥用算法 f_2 保护三级密钥，以此类推，直到最后的 n 级密钥用算法 f_n 保护明文数据。随着加密过程的进行，各层密钥的内容发生动态变化，而这种变化的规则由相应层次的密钥协议控制。其中每一层密钥又可以划分为若干种不同功能的成分，有的成分必须以密文的方式存在，有的则允许以明文的方式存在。



以上结构的基本思想就是使用密钥来保护密钥。f_i层密钥 K_i 保护，f_{i+1} 层密钥 K_{i+1} 保护，同时它本身还受到f_{i-1} 层密钥 K_{i-1} 的保护。

最低层的密钥 K_n 也叫作工作密钥，用于直接加、解密数据，而所有上层的密钥均叫作密钥加密密钥。为保证密钥的安全，一般情况下工作密钥平时并不放在加密装置里保存，而是在需要进行加、解密时由上层的密钥临时产生，使用完毕就立即清除。

最高层的密钥 K_1 也叫作主密钥。一般来说，主密钥是整个密钥管理系统中最核心、最重要的部分，应采用最保险的手段严格保护。

多层密钥体制的优点如下。

- 安全性大大提高。主要体现在下层的密钥被破译不会影响到上层密钥的安全。
- 为密钥管理自动化带来了方便。

2.2.5 密钥分发

密钥管理需解决的另一个基本问题是密钥的定期更换问题。任何密钥都应有规定的使用期限，制定使用期限的依据不是取决于在这段时间内密码能否被破译，而是从概率的意义上看密钥机密是否有可能被泄露出去。从密码技术的现状来看，现在完全可以做到使加密设备里的密钥几年内不更换，甚至在整个加密设备的有效期内保持不变。但是，加密设备里的密钥在使用多长时间后就有可能被窃取或被泄露，这个问题超出了数学的能力之外。比如一个花了 100 万美元也难以破译的密码系统也可能只需 1 万美元就能买通密钥管理人员。

显然，密钥应当尽可能地经常更换，更换密钥时应尽量减少人工干预，必要时一些核心密钥对操作人员也要保密，这就涉及密钥分发技术问题。

密钥分发技术中最成熟的方案是采用密钥分发中心(Key Distribution Center，KDC)，这是当今密钥管理的一个主流。其基本思想如下：

(1) 每个节点或用户只需保管与 KDC 之间使用的密钥加密密钥，这样的密钥配置实现了以密钥分发中心——KDC 为中心的星型通信网。

(2) 当两个用户需要相互通信时，只需向密钥分发中心申请，密钥分发中心就把加密过的工作密钥分别发送给主叫用户和被叫用户，这样对于每个用户来说就不需要保存大量的密钥了，而且真正用于加密明文的工作密钥是一报一换的，可以做到随用随申请随清除。

(3) 为保证密钥分发中心正常，还应考虑非法的第三者不能插入伪造的服务而取代密钥分发中心，这种验证身份的工作也是密钥分发中心的工作。

1. 对称密钥的分发

对称密码体制的主要特点是加/解密双方在加/解密过程中要使用完全相同的一个密钥。

对称密钥密码体制存在的最主要问题是，由于加/解密双方都要使用相同的密钥，因此在发送、接收数据之前，必须完成密钥的分发。所以，密钥的分发便成了该加密体系中的最薄弱、也是风险最大的环节。

由于公钥加密的安全性高，所以对称密钥密码体制多采用公钥加密的方法。发送方用接收方的公钥将要传递的密钥加密，接收方用自己的私钥解密传递过来的密钥，而其他人

由于没有接收方的私钥，所以不可能得到传递的密钥，这样，对称密钥密码体制的密钥在传递过程中被破解的可能性大大降低。

用一个实例来说明对称密钥密码体制的密钥分发存在的问题。例如，设有 n 方参与通信，若 n 方都采用同一个对称密钥，这样密钥管理和传递容易，可是一旦密钥被破解，整个体系就会崩溃。若采用不同的对称密钥则需 $n(n-1)$个密钥，密钥数与参与通信人数的平方数成正比，假设在某机构中有 100 个人，如果任何两个人之间需要不同的密钥，则总共需要 4950 个密钥，而且每个人应记住 99 个密钥。如果机构的人数是 1000、10000 人或更多，管理密钥将是一件可怕的事情。

为能在因特网上提供一个实用的解决方案，Kerberos 建立了一个安全的、可信任的密钥分发中心，每个用户只要知道一个和 KDC 进行会话的密钥就可以了，而不需要知道成百上千个不同的密钥。

假设用户甲想要和用户乙进行秘密通信，则甲先和 KDC 通信，用只有用户甲和 KDC 知道的密钥进行加密，用户甲告诉 KDC 他想和用户乙进行通信，KDC 会为用户甲和用户乙之间的会话随机选择一个对话密钥，并生成一个标签，这个标签用 KDC 和用户乙之间的密钥进行加密，并在用户甲启动和用户乙对话时，把这个标签交给用户乙。这个标签的作用是让用户甲确信和他交谈的是用户乙，而不是冒充者。因为这个标签是由只有用户乙和 KDC 知道的密钥进行加密的，所以即使冒充者得到用户甲发出的标签也不可能进行解密，只有用户乙收到后才能够进行解密，从而确定了与用户甲对话的人就是用户乙。

当 KDC 生成标签和随机会话密码后，就会把它们用只有用户甲和 KDC 知道的密钥进行加密，然后把标签和会话密钥传给用户甲，加密的结果可以确保只有用户甲能得到这个信息，只有用户甲能利用这个会话密钥和用户乙进行通话。同理，KDC 会把会话密码用只有 KDC 和用户乙知道的密钥加密，并把会话密钥给用户乙，如图 2.5 所示。

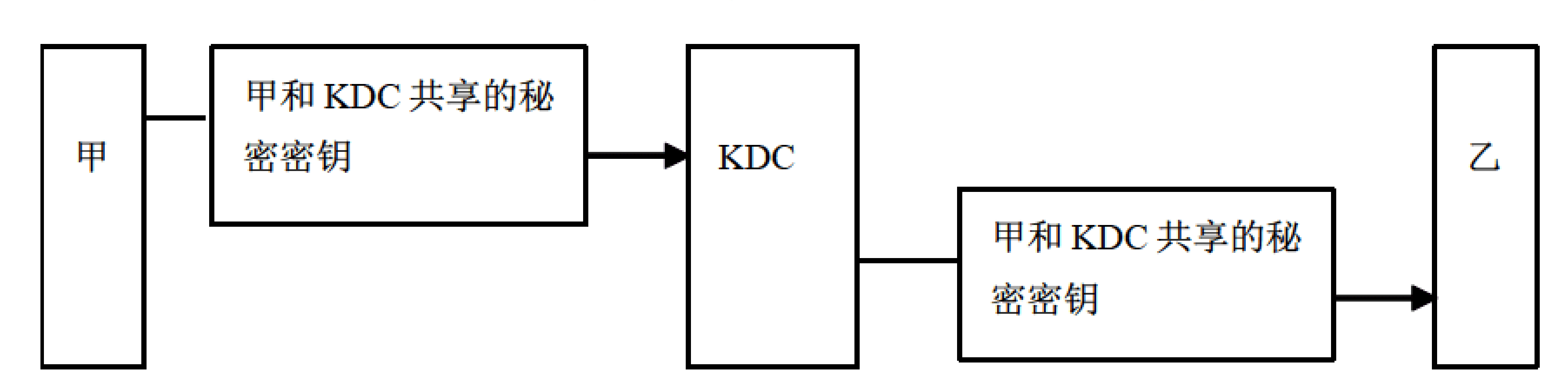


图 2.5　对称密钥的分发

用户甲会启动一个和用户乙的会话，并用得到的会话密钥加密自己和用户乙的会话，还要把 KDC 传给它的标签传给用户乙以确定用户乙的身份，然后用户甲和用户乙之间就可以用会话密钥进行安全会话了。为了保证安全，这个会话密钥是一次性的，这样黑客就更难进行破解了。同时由于密钥是一次性由系统自动产生的，则用户不必记那么多密钥，方便了人们的通信。

2. 公钥的分发

非对称密钥密码体制，即公开密钥密码体制能够验证信息发送人与接收人的真实身份，对所发出/接收信息在事后具有不可抵赖性，能够保障数据的完整性。这里有一个前提就是要保证公钥和公钥持有人之间的对应关系。因为任何人都可以通过多种不同的方式公布自己的公钥，如个人主页、电子邮件和其他一些公用服务器等，由于其他人无法确认它所公



布的公钥是否就是他自己的，所以也就无法认可他的数字签名。

如果得到了一个虚假的公钥，比如说想传给 A 一个文件，于是开始查找 A 的公钥，但是这时 B 从中捣乱，他把自己的公钥替换了 A 的公钥，让 A 错误地认为 B 的公钥就是 A 的公钥，导致最终使用 B 的公钥加密文件，结果 A 无法打开文件，而 B 可以打开文件，这样 B 实现了对保密信息的窃取行为。因此就算是采用非对称密码技术，仍旧无法完全保证保密性，那么如何才能准确地得到别人的公钥呢？这时就需要一个仲裁机构，或者说是一个权威机构，它能准确无误地提供他人的公钥，这就是 CA(Certification Authority，认证机构或认证中心)。

这实际上也是应用公钥技术的关键，即如何确认某个人真正拥有公钥(及对应的私钥)。为确保用户的身份及其所持有密钥的正确匹配，公开密钥系统需要一个值得信赖而且独立的第三方机构充当认证中心，来确认公钥拥有人的真正身份。认证中心发放一个叫作“公钥证书”的身份证明，公钥证书通常简称为证书，是一种数字签名的声明，它将公钥的值绑定到持有对应私钥的个人、设备或服务的标识上。像公安局对身份证盖章一样，认证中心利用其本身的私钥为数字证书加上数字签名，任何想发放自己公钥的用户，都可以去认证中心申请自己的证书。认证中心在核实真实身份后，颁发包含用户公钥的数字证书。其他用户只要能验证证书是真实的，并且信任颁发证书的认证中心，就可以确认用户的公钥。有了大家信任的认证中心，用户才能放心、方便地使用公钥技术带来的安全服务。

2.2.6 密钥的保护

密钥保护技术涉及密钥的装入、存储、使用、更换、销毁等多个方面，以下简要讨论密钥保护中的几个基本问题。

1. 密钥的装入

加密设备里的最高层密钥(主密钥或一级密钥)通常都需要以人工的方式装入。把密钥装入到加密设备经常采用的方式有键盘输入、软盘输入、专用的密钥装入设备(即密钥枪)输入等。密钥除了正在进行加密操作的情况以外，应当一律以加密保护的形式存放。密钥的装入过程应有一个封闭的工作环境，所有接近密钥装入工作的人员应当是绝对安全的，不存在可被窃听装置接收的电磁波或其他辐射。

采用密钥枪或密钥软盘应与键盘输入的口令相结合，只有在输入了合法的加密操作口令后才能激活密钥枪或软盘里的密钥信息，应建立一定的接口规范。

在密钥装入过程完成后，不允许存在任何可能导出密钥的残留信息，比如应将内存中使用过的存储区清零。

当使用密钥装入设备用于远距离传递密钥时，装入设备本身应设计成封闭式的物理、逻辑单元。

在可能的条件下，重要的密钥可采取由多人、多批次分开完成装入，这种方式的代价较高，但提供了多密钥的加密环境。

密钥装入的内容应不能被显示出来。为了掌握密钥装入的过程，所有的密钥应按照编号进行管理，而这些编号是公开的、可显示的。



2. 密钥的存储

在密钥装入以后，所有存储在加密设备里的密钥都应以加密的形式存放，而对这些密钥解密的操作口令应该由密码操作人员掌握。这样即使装有密钥的加密设备被破译者拿到也可以保证密钥系统的安全。

(1) 加密设备应有一定的物理保护措施。最重要的密钥信息应采用掉电保护措施，使得在任何情况下只要一拆开加密设备，这部分密钥就会自动丢失。

(2) 如果采用软件加密的形式，应有一定的软件保护措施。

(3) 重要的加密设备应有紧急情况下清除密钥的设计。

(4) 在可能的情况下，应有对加密设备进行非法使用的审计的设计，把非法口令输入等事件的产生时间等记录下来。

(5) 高级的专用加密装置应做到无论通过直观的、电子的或其他方法(X 射线、电子显微镜)都不可能从加密设备中读出信息。

(6) 对当前使用的密钥应有密钥的合法性验证措施，以防止被篡改。

3. 密钥的使用

密钥不能无限期地使用，密钥的使用时间越长，泄露的机会就越大。不同的密钥应有不同的有效期，如电话就是把通话时间作为密钥有效期，当再次通话时就启动新的密钥。密钥加密密钥无须频繁更换，因为它们只是偶尔进行密钥交换。而用来加密保存数据文件的加密密钥不能经常地交换，因为文件可以加密储藏在磁盘上数月或数年。公开密钥应用中私人密钥的有效期是根据应用的不同而变化，用于数字签名和身份识别的私人密钥必须持续数年甚至终身。

4. 密钥的更换

一旦密钥有效期到，必须清除原密钥存储区，或者用随机产生的噪声重写。但为了保证加密设备能连续工作，也可以设计成新密钥生效后，旧密钥还继续使用一段时间，以防止在更换密钥期间不能解密。

密钥更换可以采用批密钥的方式，即一次性装入多个密钥，在更换密钥时可按照一个密钥生效，另一个密钥废除的形式进行，替代的次序可采用密钥的序号。如果批密钥的生效与废除是按顺序的，那么序数低于正在使用的密钥的所有密钥都已过期，相应的存储区应清零。当为了跳过一个密钥而强制密钥更换，由于被跳过的密钥不再使用，也应执行清零。

5. 密钥的销毁

在密钥定期更换后，旧密钥就必须销毁。旧密钥是有价值的，即使不再使用，有了它们攻击者能读到由它加密的一些旧消息。要安全地销毁存储在磁盘上的密钥，应多次对磁盘存储的实际位置进行写覆盖或将磁盘切碎，用一个特殊的删除程序查看所有磁盘，寻找在未用存储区上的密钥副本，并将它们删除。



2.3 数字签名与数字证书

在传统商务活动中，为保证交易的安全与真实，一份书面合同或公文要由当事人或其负责人签字、盖章，以便让交易双方识别是谁签的合同，保证签字或盖章的人认可合同的内容，在法律上才能承认这份合同的有效性。而在电子商务的虚拟世界中，合同或文件是以电子文件的形式表现和传递的，在电子文件上，传统的手写签名和盖章是无法进行的，这就必须依靠技术手段来替代。

2.3.1 电子签名

电子签名不是书面签名的数字化，而是现代认证技术的泛称，美国《统一电子交易法》规定：电子签名泛指“与电子记录相关联的或在逻辑上相联的电子声音、符号或程序，而该电子声音、符号或程序是某人为签署电子记录的目的而签订或采用的”。联合国《电子商务示范法》中规定：电子签名是包含、附加在某一数据电文内，或逻辑上与某一数据电文相联系的电子形式的数据，它能被用来证实与此数据电文有关的签名人的身份，并表明该签名人认可该数据电文所载信息。欧盟的《电子签名指令》规定：电子签名泛指与其他电子记录相连的或在逻辑上相连并以此作为认证方法的电子形式数据。

从上述定义来看，凡是能在电子商务中，起到证明当事人的身份、证明当事人对文件内容认可的电子技术手段，都可称为电子签名，它是电子商务安全的重要保障手段。

目前，可以通过多种技术手段实现电子签名，在确认签署者的确切身份后，人们可以用多种不同的方法签署一份电子记录。方法有：手写签名或图章的模式识别；以生物特征统计学为基础的识别标识，一个让收件人能识别发件人身份的密码代号、密码或个人识别码(PIN)，基于 PKI(Public Key Infrastructure，公钥基础设施)的公钥密码技术的数字签名等。

1. 手写签名或图章的模式识别

将手写签名或印章作为图像，扫描转换后在数据库中加以存储，当对此人进行验证时，扫描输入并将原数据库中对应图像调出，用模式识别的数学计算方法进行比对，以确认该签名或印章的真伪。由于这种方法需要大容量数据库存储以及每次手写签名和盖印都有差异，因此不适用于在因特网上传输。

2. 生物识别技术

生物识别技术是利用人体生物特征进行身份认证的一种技术，生物特征是一个人与他人不同的唯一表征，它是可以测量、自动识别和验证的。生物识别系统对生物特征进行取样，提取其唯一的特征进行数字化处理，转换成数字代码，并进一步将这些代码组成特征模板存于数据库中。人们同识别系统交互进行身份认证时，识别系统获取其特征并与数据库中的特征模板进行比对，以确定是否匹配，从而确认或否认此人。以上身份识别方法适用于面对面场合，而不适用于远程网络认证及大规模人群认证。



3. 密码、密码代号或个人识别码

传统的对称密钥加/解密的身份识别和签名方法中，甲方需要乙方签署一份电子文件，甲方可产生一个随机码传送给乙方，乙方用双方事先约定好的对称密钥加密该随机码和电子文件回送给甲方，甲方用同样对称密钥解密后得到电文并核对随机码，如随机码核对正确，甲方即可认为该电文来自乙方。它适用于远程网络传输，但对称密钥管理困难，不适合大规模人群认证。

实现电子签名的技术手段有很多种，但目前比较成熟的、使用方便且具有可操作性的、在世界先进国家和我国普遍使用的电子签名技术，还是基于 PKI 的数字签名技术。由于保持技术中立性是制定法律的一个基本原则，目前还没有任何理由说明公钥密码理论是电子签名的唯一技术，因此有必要规定一个更一般化的概念以适应今后技术的发展。

在对称密钥加/解密认证中，在实际应用方面经常采用的是 ID+PIN(身份唯一标识+口令)，即发送方用对称密钥加密 ID 和 PIN 发送给接收方，接收方解密后与后台存放的 ID 和口令进行比对，达到认证的目的。人们在日常生活中使用的银行卡就采用这种认证方法。它适用于远程网络传输，对称密钥管理困难，不适用于电子签名。

2.3.2　认证机构(CA)

认证机构是 PKI 的核心执行机构，是 PKI 的主要组成部分，一般简称为 CA，在业界通常把它称为认证中心，它是具有权威性、可信任性和公正性的第三方机构。认证机构 CA 的建设要根据国家市场准入政策由国家主管部门批准，具有权威性；CA 机构本身的建设应具备条件、采用的密码算法及技术保障是高度安全的，具有可信任性；CA 是不参与交易双方利益的第三方机构，具有公正性。CA 认证机构在《电子签名法》中被称为“电子认证服务提供者”。

CA 的组成主要有：①证书签发服务器，负责证书的签发和管理，包括证书归档、撤销和更新等；②密钥管理中心，用硬件加密机产生公/私密钥对，提供 CA 证书的签发；③目录服务器负责证书和证书撤销列表(CRL)的发布和查询。

CA 的组成结构如图 2.6 所示。它是一个层次结构，第一级是根 CA(Root CA)，负责总政策；第二级是政策 CA(PCA)，负责制定具体认证策略；第三级为操作 CA(OCA)，是证书签发、发布和管理的机构。

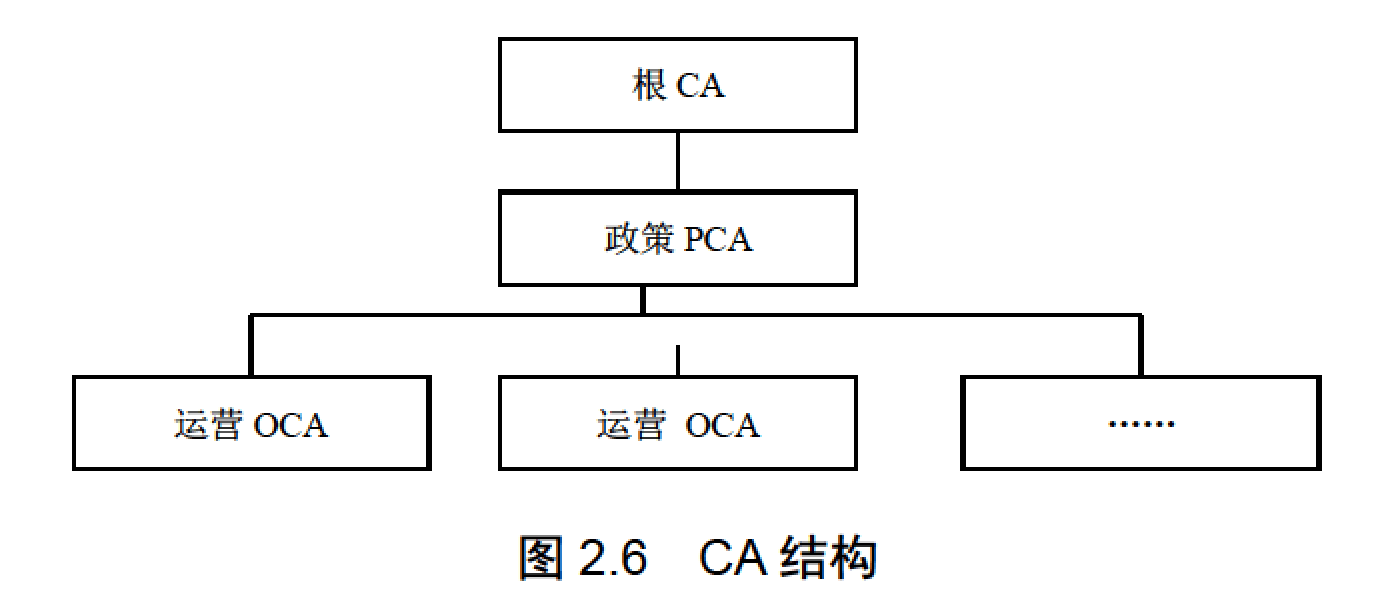


图 2.6　CA 结构

RA(Registration Authority，注册机构)是认证中心的组成部分，是数字证书的申请注册、审批、校对和管理机构。证书申请注册机构 RA 也是层次结构，RA 为注册总中心，负责证书申请注册汇总；LRA 为远程本地受理点，负责用户证书申请和审查，只有那些经过身份



信用审查合格的用户，才可以接受证书的申请，批准向其签发证书，这是保障证书使用的安全基础。

2.3.3 数字签名

数字签名在 ISO 7498-2 标准中的定义为：附加在数据单元上的一些数据，或是对数据单元所做的密码变换，这种数据和变换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性，并保护数据，防止被别人(如接收者)伪造。美国电子签名标准(DSS，FIPS186-2)对数字签名作了以下解释：“利用一套规则和一个参数对数据计算所得的结果，用此结果能够确认签名者的身份和数据的完整性”。 数字签名必须保证以下 3 点：

(1) 接收者能够核实发送者对报文的签名。

(2) 发送者事后不能抵赖对报文的签名。

(3) 接收者不能伪造对报文的签名。

可以有多种方法来实现数字签名，以下介绍其中的几种。

1. 使用秘密密钥算法的数字签名

这种方式需要 CA 的参与，每个用户事先选择好一个与 CA 共享的密钥，并亲手交到 CA 办公室，以保证只有用户和 CA 知道这个密钥。此外，CA 还有一个对所有用户都保密的密钥 K_{CA}，如图 2.7 所示。

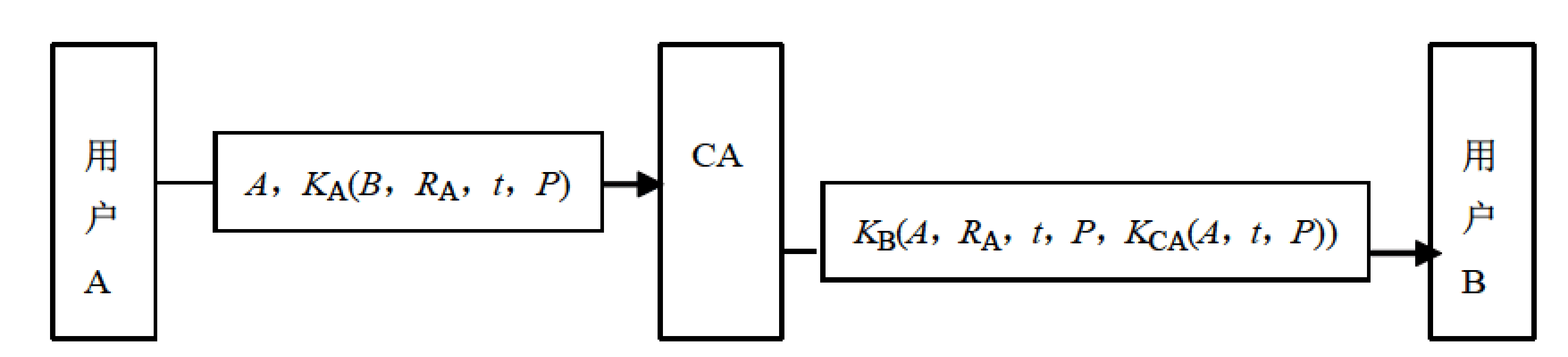


图 2.7 使用 CA 进行数字签名

当用户 A 想向用户 B 发送一个签名的报文 P 时，它向 CA 发出 $K_A(B,R_A,t,P)$，其中 R_A 为报文的随机编号，t 为时间戳；CA 将其解密后，重新组织成一个新的密文 $K_B(A,R_A,t,P,K_{CA}(A,t,P))$发给 B，因为只有 CA 知道密钥 K_{CA}，因此其他任何人都无法产生和解开密文 $K_{CA}(A,t,P)$；B 用密钥 K_B 解开密文后，首先将 $K_{CA}(A,t,P)$放在一个安全的地方，然后阅读和执行 P。

当过后 A 试图否认给 B 发过报文 P 时，B 可以出示 $K_{CA}(A,t,P)$来证明 A 确实发过 P，因为 B 自己无法伪造出 $K_{CA}(A,t,P)$，它是由 CA 发来的，而 CA 是可以信赖的，如果 A 曾给 CA 发过 P，CA 就不会将 P 发给 B，这时只要用 K_{CA} 对 $K_{CA}(A,t,P)$进行解密，一切就可真相大白。

为避免重复攻击，协议中使用了随机报文编号 R_A 和时间戳 t。B 能记住最近收到的所有报文编号，如果和其中的某个编号相同，则 P 就被当成是一个复制品而丢弃，另外 B 也根据时间戳 t 丢弃一些非常老的报文，以防止攻击者经过很长一段时间后再用老报文来重复攻击。



2. 使用公开密钥算法的数字签名

使用公开密钥算法的数字签名的加密算法和解密算法除了要满足 $D(E(P))=P$ 外，还必须满足 $E(D(P))=P$。数字签名的过程如图 2.8 所示，当用户 A 想向用户 B 发送签名的报文 P 时，它向 B 发送 $E_B(D_A(P))$，由于 A 知道自己的私人密钥 D_A 和 B 的公开密钥 E_B，因而这是可能的；B 收到密文后，先用私人密钥 D_B 解开密文，将 $D_A(P)$复制一份放于安全的地方，然后用 A 的公开密钥 E_A 将 $D_A(P)$解开，取出 P。如图 2.8 所示。

当 A 过后试图否认给 B 发过 P 时，B 可以出示 $D_A(P)$作为证据，因为 B 没有 A 的私人密钥 D_A，除非 A 确实发过 $D_A(P)$，否则 B 是不会有这样一份密文的，只要用 A 的公开密钥 E_A 解开 $D_A(P)$，就可以知道 B 说的是真话。

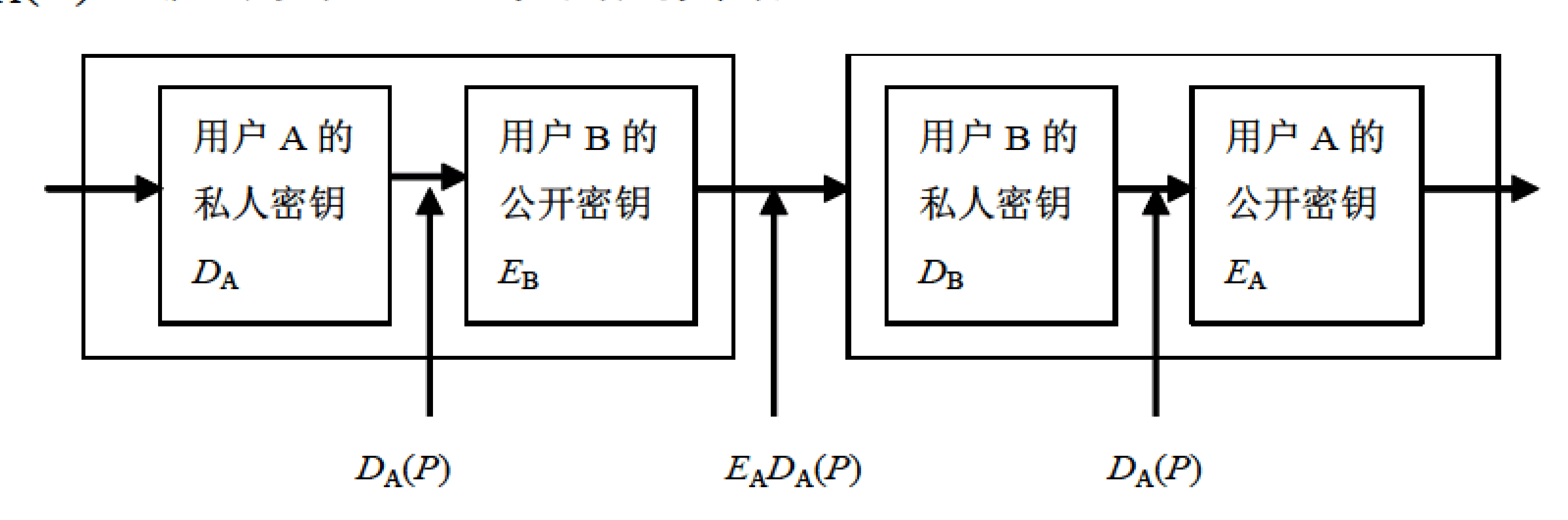


图 2.8　使用公开密钥的数字签名

3. 使用报文摘要的数字签名

以上的签名方法将认证和保密两种截然不同的功能混在了一起，有些报文只需要签名而不需要保密。为此有人提出一个新的方案，使用一个单向的 Hash 函数，将任意长的明文转换成一个固定长度的数据串，然后仅对该数据串进行加密。

这样的 Hash 函数通常称为报文摘要(Message Digests，MD)，它必须满足以下 3 个条件：

(1)　给定 P 就很容易计算出 MD(P)。

(2)　只给出 MD(P)，很难计算出 P。

(3)　无法生成两个具有相同的报文摘要的报文。

为满足第③个条件，MD(P)至少必须达到 128bit，实际上有很多函数符合以上 3 个条件。

考虑图 2.8 的例子，CA 解开密文后，首先计算出 MD(P)，然后着手组织一个新的密文，在新的密文中它不是发送 $K_{CA}(A，t，P)$，而是发送 $K_{CA}(A，t，\text{MD}(P))$，而 B 解开密文后将 $K_{CA}(A，t，\text{MD}(P))$保存起来。如果发生纠纷，B 可以出示 P 和 $K_{CA}(A，t，\text{MD}(P))$作为证据。

因为 $K_{CA}(A，t，\text{MD}(P))$是由 CA 送来的，B 无法伪造，当 CA 用 K_{CA} 解开密文取出 MD(P)后，可将 Hash 函数作用于 B 提供的明文 P，然后判断报文摘要是否和 MD(P)相同。因为条件③保证了不可能伪造出另一个报文，使得其报文摘要同 MD(P)一样，因此只要两个报文摘要相同，就证明了 B 确实收到了 P。

在公开密钥密码系统中，使用报文摘要进行数字签名的过程如图 2.9 所示。首先用户 A 对明文 P 计算出 MD(P)，然后用私人密钥对 MD(P)进行加密，连同明文 P 一起发送给用户 B；B 将 $D_A(\text{MD}(P))$复制一份放于安全的地方，然后用 A 的公开密钥解开密文取出 MD(P)，为防止途中有人更换报文 P，B 对 P 进行报文摘要，如结果同 MD(P)相同，则将 P 接收下



来。当 B 试图否认发送过 P 时，B 可以出示 P 和 $D_A(MD(P))$来证明自己确实收到过 P。

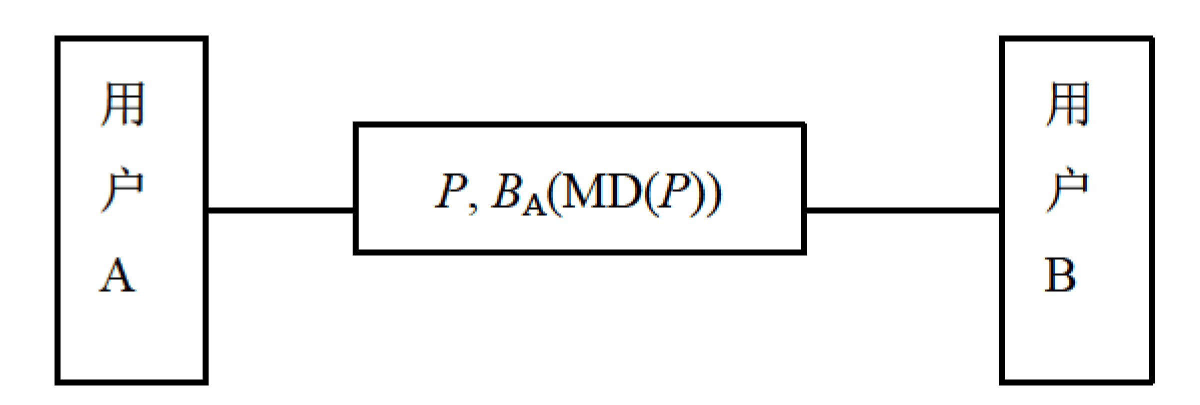


图 2.9　使用报文摘要的数字签名

以上就是实现数字签名的方法，在这几种方法中，使用公开密钥的数字签名应用最广，通常说的数字签名就是指使用公开密钥的数字签名。

2.3.4　公钥基础设施(PKI)

使用数字签名的前提就是要保证公钥和公钥持有人之间的对应关系，即如何确认某个人是否真正拥有公钥(及对应的私钥)。为解决这个问题，世界各国对其进行了多年的研究，初步形成了一套完整的 Internet 安全解决方案，即目前被广泛采用的 PKI 技术(Public Key Infrastructure，公钥基础设施)技术。该技术采用证书管理公钥，通过第三方的可信任机构——认证中心(CA)，把用户的公钥和其他标识信息(如名称、E-mail、身份证号等)捆绑在一起，在 Internet 上验证用户的身份。目前，通用的办法是采用基于 PKI 结构结合数字证书，通过把要传输的数字信息进行加密，保证信息传输的保密性、完整性，签名保证身份的真实性和抗抵赖性。

PKI 是一个利用非对称密码算法(即公开密钥算法)原理和技术实现并提供网络安全服务的通用安全基础设施，它遵循标准的公钥加密技术，为电子商务、电子政务、网上银行和网上证券业，提供一整套安全保证的基础平台。PKI 这种遵循标准的密钥管理平台，能够为所有网上应用提供加/解密和数字签名等安全服务所需要的密钥和证书管理。

PKI 的核心执行机构是认证机构 CA，其核心元素是数字证书。

1. PKI 的标准与协议

与 PKI 相关的标准包括以下内容。

1)　X.209(1988)ASN.1 基本编码规则的规范

ASN.1 用于描述网络上传输信息的格式。它包含两部分：第一部分(ISO 8824/ITU X.208)描述信息内的数据、数据类型及序列格式，也就是数据的语法；第二部分(ISO 8825/ITU X.209)描述如何将各部分数据组成消息，也就是数据的基本编码规则。

ASN.1 原来是作为 X.409 的一部分而开发的，后来独立地成为一个标准。这两个协议除了在 PKI 体系中被应用外，还被广泛应用于通信和计算机等其他领域。

2)　X.500(1993)信息技术(开放系统互联)的概念、模型及服务简述

X.500 是一套已经被国际标准化组织(ISO)接受的目录服务系统标准，它定义了一个机构如何在全局范围内共享其名字和与之相关的对象。X.500 是层次性的，其中的管理性域(机构、分支、部门和工作组)可以提供这些域内的用户和资源信息。在 PKI 体系中，X.500 被用来唯一标识一个实体，该实体可以是机构、组织、个人或一台服务器。X.500 被认为是实现目录服务的最佳途径，但 X.500 的实现需要较大的投资，并且比其他方式速度慢；而



其优势则在于具有信息模型、多功能和开放性。

3)　X.509(1993)信息技术(开放系统互联)的鉴别框架

X.509 是由国际电信联盟(ITU-T)制定的数字证书标准。在 X.500 确保用户名称唯一性的基础上，X.509 为 X.500 用户名称提供通信实体的鉴别机制，并规定实体鉴别过程中广泛适用的证书语法和数据接口。

X.509 证书由用户公共密钥和用户标识符组成，此外还包括版本号、证书序列号、CA 标识符、签名算法标识、签发者名称及证书有效期等信息。这一标准的最新版本是 X.509 v3。

2. PKCS 系列标准

由 RSA 实验室制定的 PKCS 系列标准，是一套针对 PKI 体系的加/解密、签名、密钥交换、分发格式的行为标准，该标准目前已经成为 PKI 体系中不可缺少的一部分。

3. 在线证书状态协议(OCSP)

OCSP(Online Certificate Status Protocol，在线证书状态协议)是 IETF 颁布的用于检查数字证书在某一交易时刻是否仍然有效的标准。该标准提供给 PKI 用户一条方便、快捷的数字证书状态查询通道，使 PKI 体系能够更有效、更安全地在各个领域中被广泛应用。

4. 轻量级目录访问协议(LDAP)

LDAP 规范(RFC1487)简化了复杂的 X.500 目录访问协议，并且在功能性、数据表示、编码和传输方面都进行了相应的修改。1997 年，LDAP 第 3 版本成为因特网标准。目前，LDAP v3 已经在 PKI 体系中被广泛应用于证书信息发布、CRL 信息发布、CA 政策以及与信息发布相关的各个方面。

除了以上协议外，还有一些构建在 PKI 体系上的应用协议，这些协议是 PKI 体系在应用和普及化方面的代表，包括 SET 协议和 SSL 协议。

目前 PKI 体系中已经包含了众多的标准和标准协议，随着 PKI 技术的不断进步和完善，以及其应用的不断普及，将来还会有更多的标准和协议加入其中。

2.3.5　数字证书

数字证书简称证书，是 PKI 的核心元素，由认证机构服务器签发，它是数字签名的技术基础保障，符合 X.509 标准，能够证明某一实体的身份以及其公钥的合法性及该实体与公钥二者之间的匹配关系。证书是公钥的载体，证书上的公钥与实体身份唯一绑定。现行的 PKI 机制一般为双证书机制，即一个实体应具有两个证书，两个密钥对，一个是加密证书，一个是签名证书，加密证书原则上是不能用于签名的。

1. 数字证书的内容

证书在公钥体制中是密钥管理的介质，不同的实体可通过证书来互相传递公钥，证书由具有权威性、可信任性和公正性的第三方机构签发，是具有权威的电子文档。证书的主要内容，按 X.509 标准规定其逻辑表达式为

CA《A》=CA{V,SN,AI,CA,UCA,A,UA,Ap,Ta}



其中的参数说明如下。

- CA《A》：认证机构 CA 为用户 A 颁发的证书。
- CA{, , ,}：认证机构 CA 对花括弧内证书内容进行的数字签名。
- V：证书版本号。
- SN：证书序列号。
- AI：用于对证书进行签名的算法标识。
- CA：签发证书的 CA 机构的名字。
- UCA：签发证书的 CA 的唯一标识符。
- A：用户 A 的名字。
- UA：用户 A 的唯一标识。
- Ap：用户 A 的公钥。
- Ta：证书的有效期。

从 V 到 Ta 是证书在标准域中的主要内容。表 2.4 给出了一般证书的例子。

表 2.4 数字证书实例

项 目	实 例
证书格式版本	V3
证书序列号	14 c3 2a 43 7d 06 88 ec 0d 82 b2 6d c5 73 85 02
CA 签名算法标识	md5RSA
签发 CA 名称	O=cfca， c=CN
证书有效期	2005-5-1**2007-5-1
证书持有者名称	Cn=******o=cfcac=CN
证书公钥	A058.cf31.3bc3
证书扩展域	Keyusage=digital
CA 对证书的签名	Ca58.b2c3.1bc6

证书的这些内容主要用于身份认证、签名的验证和有效期的检查。CA 签发证书时，要对上述内容进行签名，以示对所签发证书内容的完整性、准确性负责，并证明该证书的合法性和有效性，最后将网上身份与证书绑定。CA 对证书的签名如图 2.10 所示。

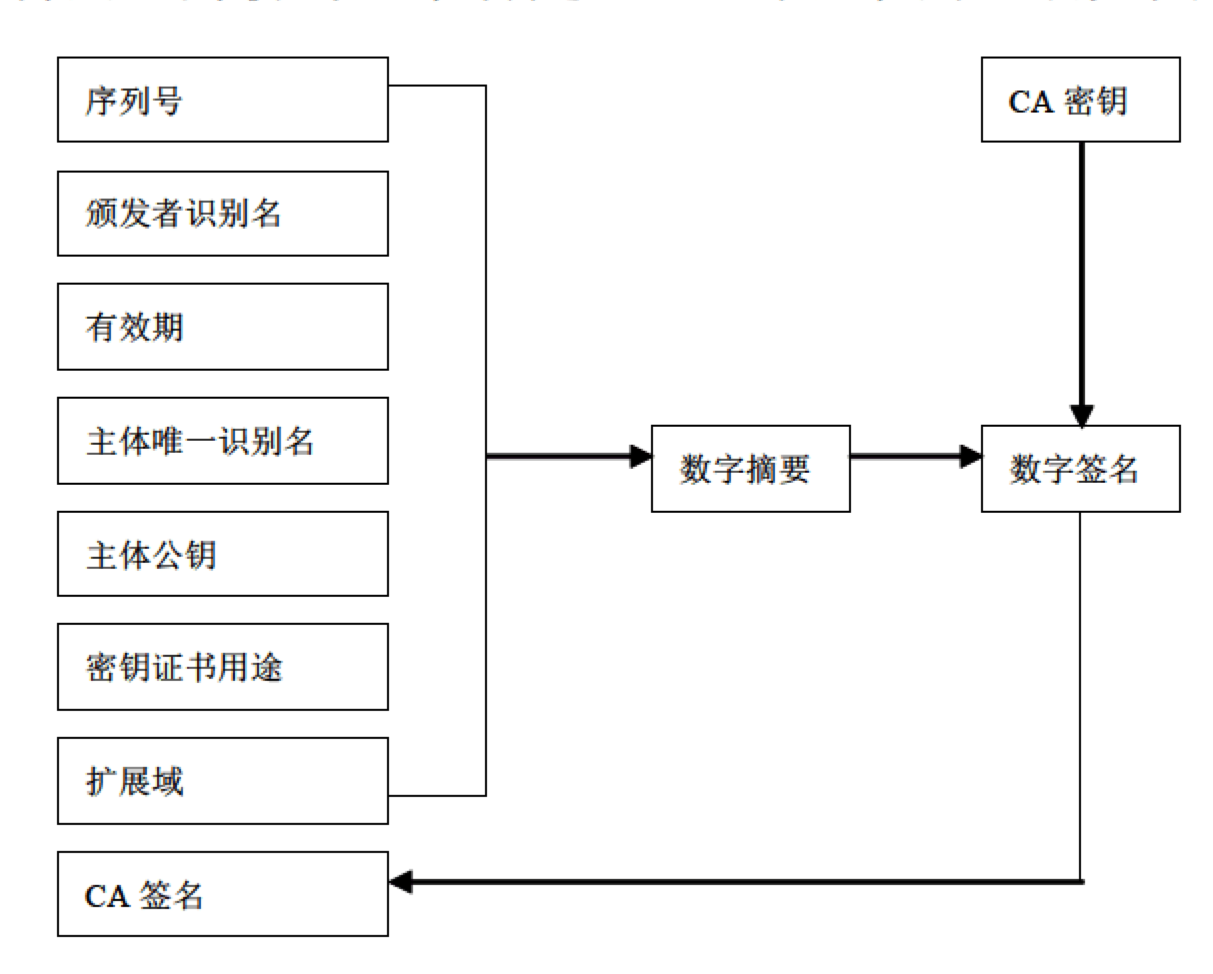


图 2.10 CA 对实体签发的证书

CA 颁发的上述证书与对应的私钥存放在一个保密文件里，最好的办法是存放在 IC 卡和 USBKey 介质中，可以保证私钥不出卡(所有的和私钥相关的密码操作均在卡内完成，充分保证根密钥的安全)，证书不能被复制，其特点是安全性高、携带方便、便于管理。

2. 数字证书的分类

数字证书通常分为个人证书、企业证书、软件证书。

(1) 个人证书(Personal Digital ID)为某一个用户提供证书，以帮助个人在网上安全地进行电子交易操作。个人身份的数字证书通常是安装在客户端的浏览器内，并通过安全的电子邮件进行交易操作。网景公司的“导航者”浏览器(Navigator)和微软公司的“探索者”浏览器(Internet Explorer)都支持该功能。个人数字证书是通过浏览器来申请获得的，认证中心对申请者的电子邮件地址、个人身份证及信用卡号等进行核实后，就签发个人数字证书，并将数字证书安置在用户所用的浏览器或电子邮件的应用系统中，同时也给申请者发送一个通知。个人数字证书的使用方法是集成在用户的浏览器的相关功能中，用户其实只要作出相应的选择就行了。

个人数字证书有 4 个级别。第一级别是最简单的，只提供个人电子邮件地址的认证，它仅与电子邮件地址有关，并不对个人信息进行认证，是最初级的认证；第二级别提供个人姓名、个人身份(驾照、社会保险号、出生年月等)等信息的认证；第三个级别是在第二级别之上加上了充当信用支票的功能；第四级别包括证书所有人的职位、所属组织等，但这一级别还没有最后定型。

(2) 企业证书，也就是服务器证书(Server ID)，它是对网上的服务器提供一个证书，拥有 Web 服务器的企业就可以用具有证书的 Internet 网站(Web Site)来进行安全电子交易。拥有数字证书的服务器可以自动与客户进行加密通信，有证书的 Web 服务器会自动地将其与客户端 Web 浏览器通信的信息加密。服务器的拥有者(相关的企业或组织)有了证书，就可以进行安全电子交易。

服务器证书的发放较为复杂。因为服务器证书是一个企业在网络上的形象，是企业在网络空间信任度的体现。权威的认证中心对每一个申请者都要进行信用调查，包括企业基本情况、营业执照、纳税证明等。要对该企业对服务器的管理情况进行考核，一般是通过事先准备好的详细验证步骤逐步进行，如是否有一套完善的管理规范，是否有完善的加密技术和保密措施，是否有多层逻辑访问控制、生物统计扫描仪、红外线监视器等，认证中心经过考察后决定是否发放或撤销服务器数字证书。一旦决定发放后，该服务器就可以安装认证中心提供的服务器证书，安装成功后即可投入服务。服务器得到数字证书后，就会有一对密钥，它与服务器是密不可分的，数字证书与这对密钥一起表示该服务器的身份，是整个认证的核心。

(3) 软件(开发者)证书(Developer ID)通常为因特网中被下载的软件提供证书，该证书用于和微软公司 Authenticode 技术(合法化软化)结合的软件，以使用户在下载软件时能获得所需的信息。

上述 3 类证书中前两类是常用的证书，第 3 类则用于较特殊的场合，大部分认证中心提供前两类证书，能完全提供各类证书的认证中心并不普遍。

数字证书的管理包括两方面的内容：一是颁发数字证书；二是撤销数字证书。在一些



情况下，如密钥丢失或被窃，或者某个服务器变更了，就需要一种方法来验证数字证书的有效性，要建立一份证书取消清单并公之于众，这份清单是可伸缩的。由于数字证书也要有相应的有效期，为此，认证中心一般都制定相应的管理措施和政策，来管理其属下的数字证书。

目前，数字证书可用于电子邮件、电子贸易、电子基金转移等各种用途。当然数字证书的应用范围和效果目前还是有限的。

2.3.6 数字时间戳技术

数字时间戳技术是数字签名技术的一种变相应用。在书面合同中，文件签署的日期和签名同样是防止文件被伪造和篡改的关键性内容。数字时间戳(Digital Time Stamp，DTS) 服务是网上电子商务安全服务项目之一，能提供电子文件的日期和时间信息的安全保护。

时间戳(Time-Stamp)是一个经加密后形成的凭证文档，它包括以下 3 个部分：

- 需加时间戳的文件的摘要(Digest)。
- DTS 收到文件的日期和时间。
- DTS 的数字签名。

用户首先将需要加时间戳的文件用 Hash 函数加密形成摘要，然后将该摘要发送到 DTS，DTS 在加入了收到文件摘要的日期和时间信息后再对该文件加密(数字签名)，然后送回用户。

书面签署文件的时间是由签署人自己写上的，而数字时间戳则不然，它是由认证单位的 DTS 来加的，以 DTS 收到文件的时间为依据。

2.4 认 证 技 术

在网络系统中，安全目标的实现除了采用加密技术外，另一个重要方面就是认证技术。认证技术的主要作用是进行信息认证。信息认证的目的：一是确认信息发送者的身份；二是验证信息的完整性，即确认信息在传送或存储过程中未被篡改过。常用的安全认证技术主要有数字摘要、数字信封、数字签名、数字时间戳、数字证书和安全认证机构等。认证是防止主动攻击的重要技术，它对于开放环境中的各种信息系统的安全有重要作用。

认证技术一般可以分为以下两种。

(1) 身份认证。用于鉴别用户身份，包括识别，明确并区分访问者的身份；验证，对访问者声称的身份进行确认。

(2) 消息认证。用于保证信息的完整性和抗否认性。在很多情况下，用户要确认网上信息是不是假的，信息是否被第三方修改或伪造，这就需要消息认证。消息认证的有关内容参见加密、解密部分和数字签名部分。

2.4.1 身份认证的重要性

有这样一个经典的漫画，一条狗在计算机面前一边打字一边对另一条狗说：“在因特网上，没有人知道你是一个人还是一条狗！”这个漫画说明了在因特网上很难识别身份。

身份认证是安全系统中的第一道关卡，如图 2.11 所示。

用户在访问安全系统之前，首先经过身份认证系统识别身份，然后访问监控器，根据用户的身份和授权数据库决定用户是否能够访问某个资源。

授权数据库由安全管理员按照需要进行配置。

审计系统根据审计设置记录用户的请求和行为，同时利用入侵检测系统实时或非实时地检测是否有入侵行为。

访问控制和审计系统都要依赖于身份认证系统提供的“信息”——用户的身份。

可见身份认证在安全系统中的地位极其重要，是最基本的安全服务，其他的安全服务都要依赖于它。一旦身份认证系统被攻破，那么系统的所有安全措施将形同虚设。黑客攻击的目标往往就是身份认证系统。

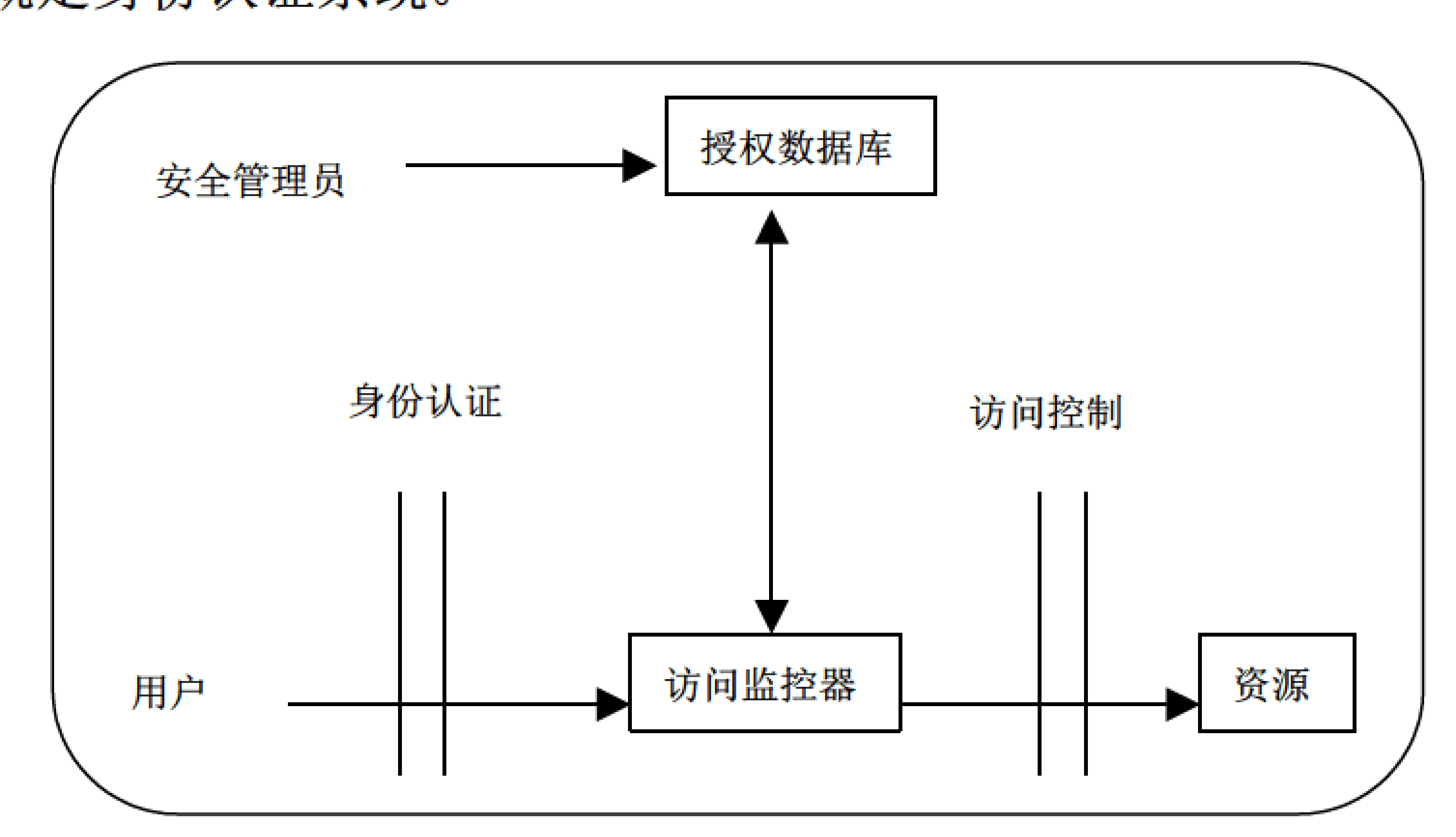


图 2.11　安全系统的逻辑结构

2.4.2　身份认证的方式

用户与主机之间的认证可以基于以下一个或几个因素。

(1)　用户所知道的东西，如口令。

(2)　用户拥有的东西，如智能卡。

(3)　用户所具有的生物特征，如指纹、声音、视网膜扫描等。

1. 基于口令的认证方式

基于口令的认证方式是最常用的一种技术，但因为它是一种单因素的认证，安全性仅依赖于口令，口令一旦泄露，用户即可被冒充。更严重的是用户往往选择简单、易被猜测的口令，如采用与用户名相同的口令以及生日、单词等，此问题往往成为安全系统最薄弱的突破口。

口令大都经过加密后存放在口令文件中，一旦口令文件被窃取，那么就可以进行离线的字典式攻击，这也是黑客最常用的手段之一。为了使口令更加安全，可以通过加密口令，或修改加密方法来提供更复杂的口令，这就是一次性口令方案。

2. 基于智能卡的认证方式

智能卡具有硬件加密功能，有较高的安全性。每个用户持有一张智能卡，智能卡存储



用户个性化的秘密信息，同时在验证服务器中也存放该秘密信息。进行认证时，用户输入PIN(个人身份识别码)，智能卡认证 PIN 成功后，即可读出智能卡中的秘密信息，进而利用该秘密信息与主机之间进行认证。

基于智能卡的认证方式是一种双因素的认证方式(PIN+智能卡)，即使 PIN 或智能卡被窃取，用户仍不会被冒充。智能卡提供硬件保护措施和加密算法，可以利用这些功能加强安全性能。例如，可以把智能卡设置成用户只能得到加密后的某个秘密信息，从而防止秘密信息的泄露。

3. 基于生物特征的认证方式

这种认证方式利用人体唯一的、可靠的、稳定的生物特征(如指纹、视网膜、声音、脸部、掌纹等)，采用计算机的强大功能和网络技术进行图像处理和模式识别。该技术具有很强的安全性和可靠性，与传统的身份确认手段相比，无疑发生了质的飞跃。近几年来，全球的生物识别技术已从研究阶段转向应用阶段，前景十分广阔。

生物识别技术主要有以下几种。

(1) 指纹识别技术。每个人的指纹皮肤纹路都是唯一的，并且终身不变，通过将指纹和预先保存在数据库中的指纹采用指纹识别算法进行比对，便可验证真实身份。

(2) 视网膜识别技术。视网膜识别技术利用激光照射眼球的背面，扫描摄取几百个视网膜的特征点，经数字化处理后形成记忆模板存储于数据库中，供以后进行比对验证。视网膜是一种极其稳定的生物特征，属于精确度较高的识别技术。

(3) 声音识别技术。声音识别技术是一种行为识别技术，用声音录入设备反复不断地测量、记录声音波形变化，进行频谱分析，经数字化处理后做成声音模板加以存储。使用时将现场采集到的声音同登记过的声音模板进行精确匹配，以识别身份。

2.4.3 消息认证

消息认证的内容包括以下几个方面。

(1) 证实消息的信源和信宿。

(2) 消息内容是否受到偶然或有意的篡改。

(3) 消息的序号和时间性。

对一个电子文件进行数字签名并在网上传输，首先要在网上进行身份认证，然后再进行签名，最后是对签名的验证。

1. 认证

PKI 提供的服务首先是认证，即身份识别，确认实体即为自己所声明的实体。认证的前提是甲乙双方都具有第三方 CA 所签发的证书，认证分单向认证和双向认证。

(1) 单向认证。单向认证是甲乙双方在网上通信时，甲只需要认证乙的身份即可。这时甲需要获取乙的证书，获取的方式有两种，一种是在通信时乙直接将证书传送给甲，另一种是甲向 CA 目录服务器索取。甲获得乙的证书后，首先用 CA 的根证书公钥验证该证书的签名，验证通过说明该证书是有效证书。然后检查证书的有效期以及该证书是否已作废(LRC 检查)，若作废则进入黑名单。

(2) 双向认证。双向认证是甲乙双方在网上通信时，用户甲不但要认证用户乙的身份，乙也要认证甲的身份。其认证过程与单向认证过程相同，如图 2.12 所示。

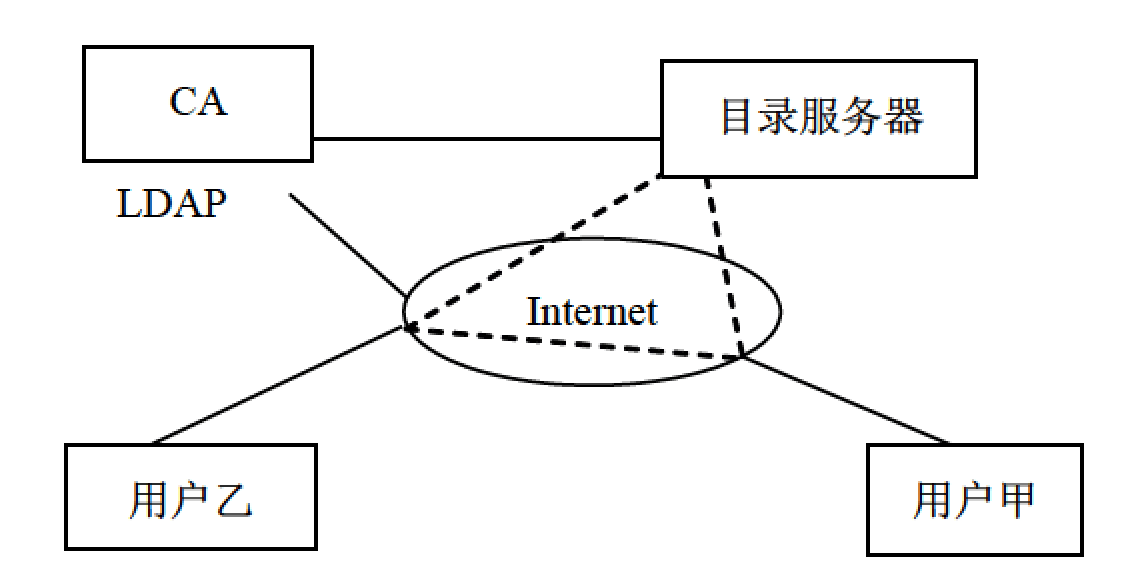


图 2.12　双向认证过程

甲乙双方在网上查询对方证书的有效性及黑名单时，采用的是 LDAP(Light Directory Access Protocol)协议，它是一种轻型目录访问协议。

2. 数字签名与验证过程

网上通信的双方，在互相认证身份后，即可发送签名的数据电文。数字签名与验证的过程和技术实现的原理如图 2.13 所示。

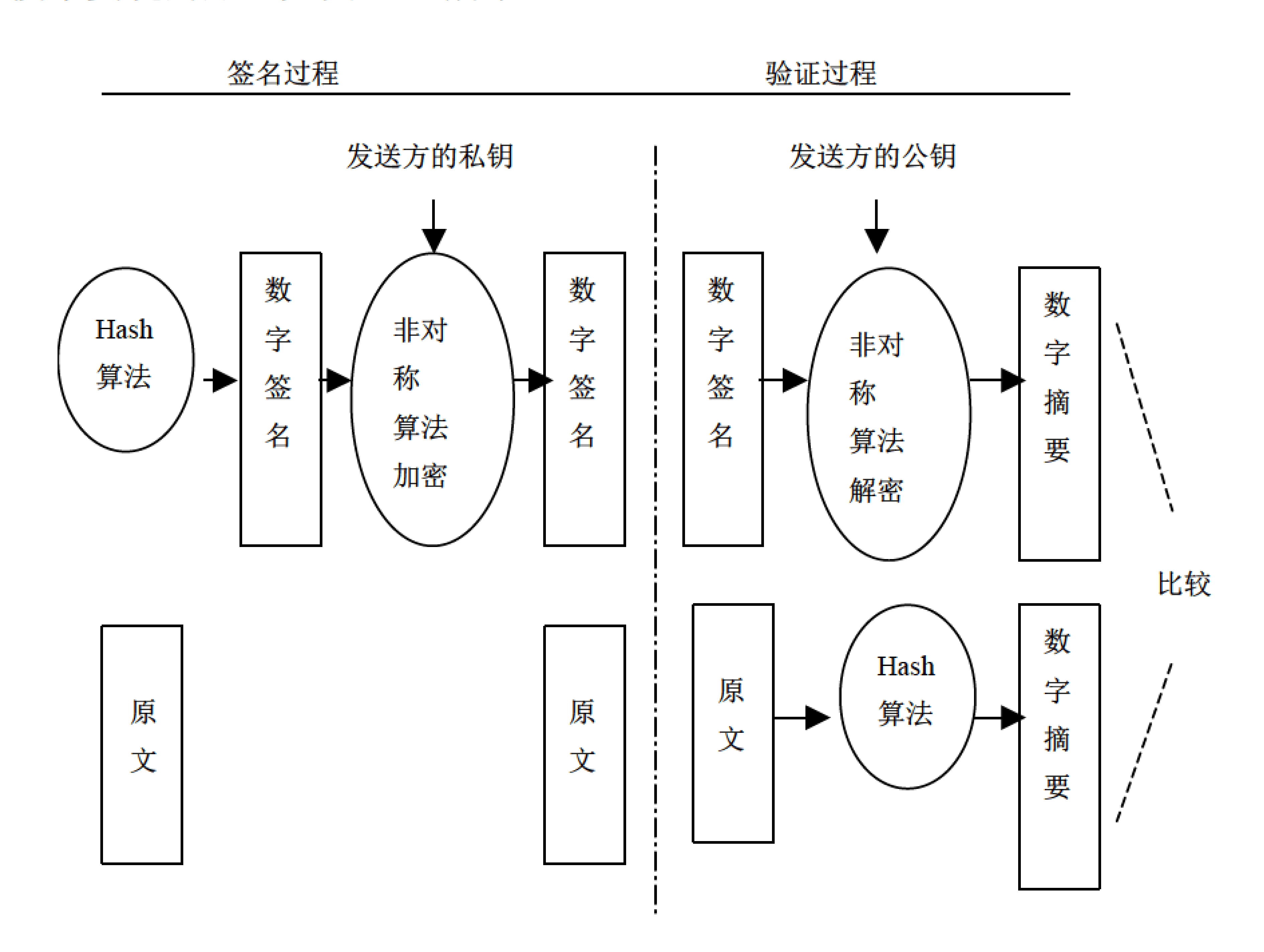


图 2.13　数字签名过程

数字签名过程分两部分，左侧为签名，右侧为验证过程。即发送方将原文用 Hash 算法求得数字摘要，用签名私钥对数字摘要加密形成数字签名，发送方将原文与数字签名一起发送给接收方；接收方验证签名，即用发送方公钥解密数字签名，获得数字摘要；然后将原文采用同样 Hash 算法又得到一个新的数字摘要，将两个数字摘要进行比较，如果二者匹配，则说明经数字签名的电子文件传输成功。



3. 数字签名的操作过程

数字签名的操作过程如图 2.14 所示，它需要有发送方的签名证书的私钥及其验证公钥。

数字签名操作具体过程如下，首先生成被签名的电子文件，然后对电子文件用 Hash 算法做数字摘要，再对数字摘要用签名私钥做非对称加密，即制作数字签名；然后将以上的签名和电子文件原文，以及签名证书的公钥加在一起进行封装，形成签名结果发送给接收方，等待接收方验证。

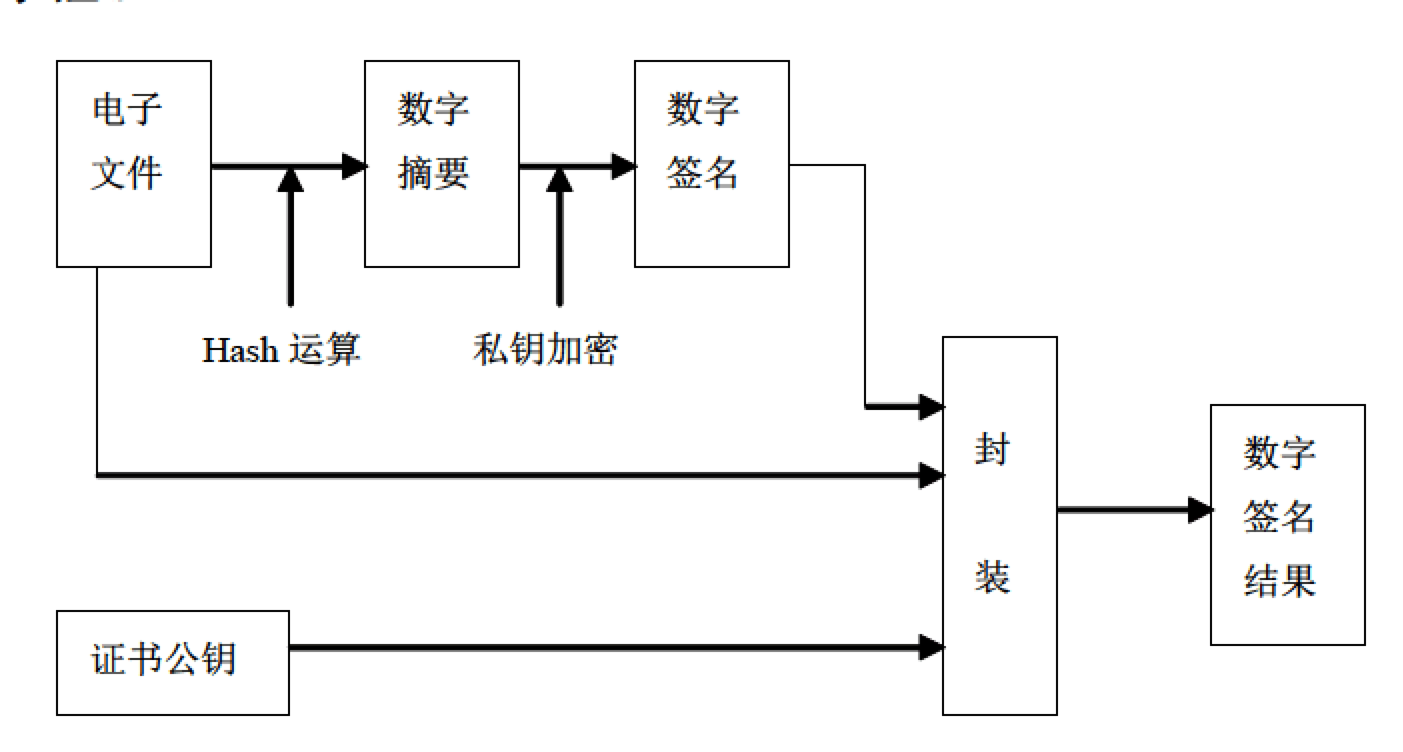


图 2.14　数字签名操作过程

4. 数字签名的验证过程

接收方收到发送方的签名结果后进行签名验证，其具体操作过程如图 2.15 所示。

接收方收到数字签名的结果，其中包括数字签名、电子原文和发送方公钥，即待验证的数据。接收方进行签名验证。验证过程是：接收方首先用发送方公钥解密数字签名，导出数字摘要，并对电子文件原文做同样 Hash 算法得出一个新的数字摘要，将两个摘要的 Hash 值进行结果比较，相同签名得到验证，否则无效。这就做到了《电子签名法》中所要求的对签名不能改动，对签署的内容和形式也不能改动的要求。

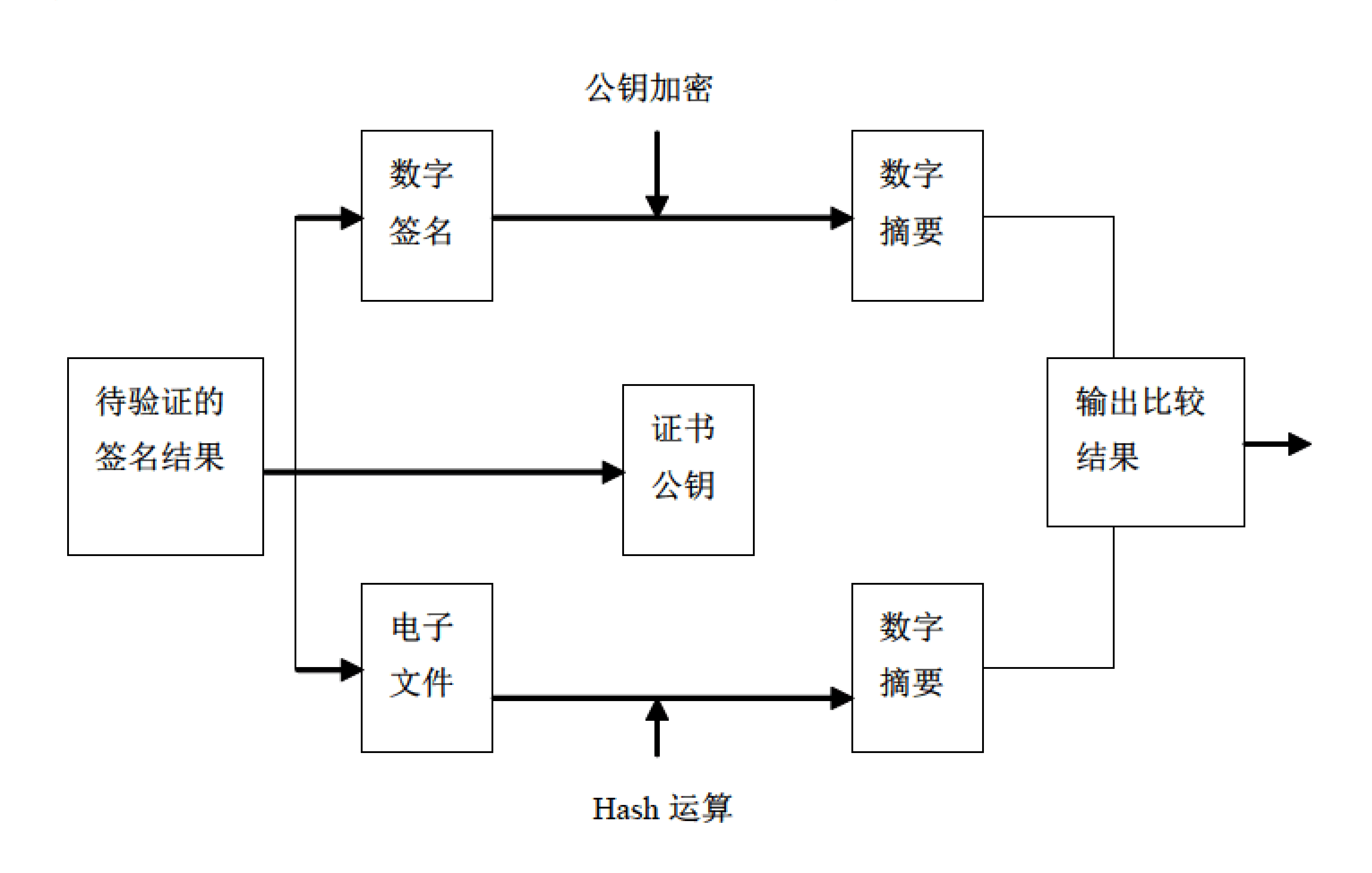


图 2.15　数字签名验证过程

5. 数字签名的作用

如果接收方对发送方数字签名验证成功，就可以说明以下 3 个实质性的问题。

(1) 该电子文件确实是由签名者即发送方所发出的，因为签署时电子签名数据由电子签名人所控制。

(2) 被签名的电子文件确实是经发送方签名后发送的，说明发送方用了自己的私钥做的签名，并得到验证。

(3) 接收方收到的电子文件在传输中没有被篡改，保持了数据的完整性，因为签署后对电子签名的任何改动都能够被发现。

6. 原文保密的数字签名的实现方法

在上述数字签名原理中定义的是对原文做数字摘要和签名并传输原文，在很多场合传输的原文是要求保密的，这就要涉及“数字信封”的概念。

数字信封的功能类似于普通信封。普通信封在法律的约束下保证只有收信人才能阅读信的内容；数字信封则采用密码技术保证了只有规定的接收人才能阅读信息的内容。

数字信封中采用单钥密码体制和公钥密码体制。信息发送者首先利用随机产生的对称密码加密信息，再利用接收方的公钥加密对称密码，被公钥加密后的对称密码称为数字信封。在传递信息时，信息接收方要解密信息时，必须先用自己的私钥解密数字信封，得到对称密码，才能利用对称密码解密所得到的信息。这样就保证了数据传输的真实性和完整性。

数字信封是信息发送端用接收端的公钥，将一个通信密钥(Symmentric Key)加密后，只有指定的接收端才能打开信封，取得秘密密钥(SK)，用它来解开传送来的信息。

签名过程请参照图 2.16。

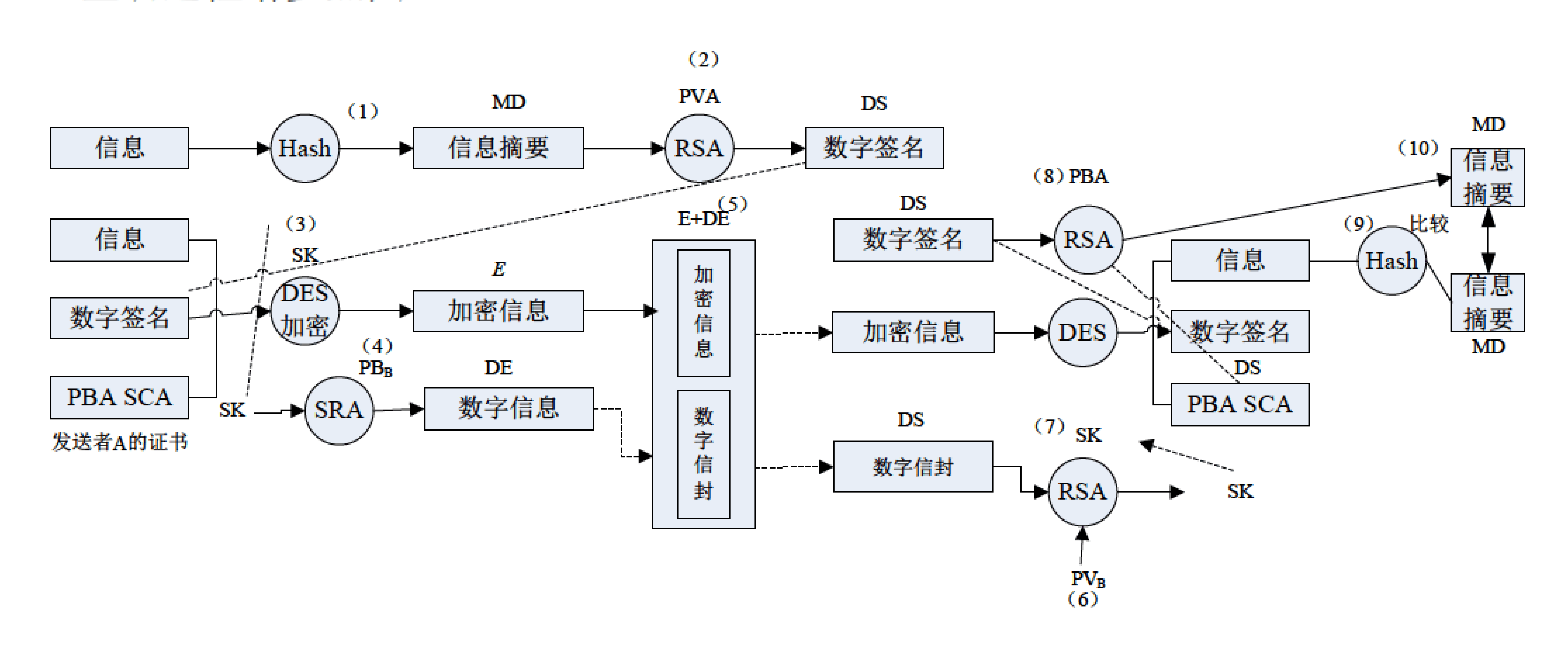


图 2.16　“数字信封”处理过程

如图 2.16 所示的流程是一个典型的“数字信封”处理过程。其基本原理是将原文用对称密钥加密传输，而将对称密钥用接收方公钥加密发送给对方。接收方收到数字信封后，用自己的私钥解密信封，取出对称密钥解密得到原文。其详细过程如下：

(1) 发送方 A 将原文信息进行 Hash 运算，得一 Hash 值即数字摘要 MD。

(2) 发送方 A 用自己的私钥 PVA，采用非对称 RSA 算法，对数字摘要 MD 进行加密，即得数字签名 DS。

(3) 发送方 A 用对称算法 DES 的对称密钥 SK 对原文信息、数字签名 SD 及发送方 A



证书的公钥 PBA 采用对称算法加密，得加密信息 E。

(4) 发送方用接收方 B 的公钥 PBB，采用 RSA 算法对对称密钥 SK 加密，形成数字信封 DE，就好像将对称密钥 SK 装到了一个用接收方公钥加密的信封里。

(5) 发送方 A 将加密信息 E 和数字信封 DE 一起发送给接收方 B。

(6) 接收方 B 接收到数字信封 DE 后，首先用自己的私钥 PVB 解密数字信封，取出对称密钥 SK。

(7) 接收方 B 用对称密钥 SK 通过 DES 算法解密加密信息 E，还原出原文信息、数字签名 SD 及发送方 A 证书的公钥 PBA。

(8) 接收方 B 验证数字签名，先用发送方 A 的公钥解密数字签名得数字摘要 MD'。

(9) 接收方 B 同时将原文信息用同样的 Hash 运算，求得一个新的数字摘要 MD。

(10) 将两个数字摘要 MD 和 MD'进行比较，验证原文是否被篡改。如果二者相等，说明数据没有被篡改，是保密传输的，签名是真实的；否则拒绝该签名。

这样就做到了敏感信息在数字签名的传输中不被篡改，未经认证和授权的人看不见原数据，从而在数字签名传输中保护了敏感数据。

2.4.4 认证技术的实际应用

认证机制分为两类，即简单认证机制和强化认证机制。简单的认证中只有名字和口令被服务系统所接受。由于明文密码在网上传输极易被获取，一般的解决办法是使用一次性口令(One-Time Password，OTP)机制。这种机制的最大优势是不必在网上传输用户的真实口令，并且使用一次后立即失效，可以有效防止重复攻击(Replay Attack)。RADIUS 协议就是属于这种类型的认证协议；强化认证机制一般将运用多种加密手段来保护认证过程中相互交换的信息，其中，Kerberos 协议是此类认证协议中比较完善的协议，得到了广泛的应用。

下面介绍几种常用的身份认证机制，并分析它们的安全性。

1. RADIUS 认证机制

RADIUS(Remote Authentication Dial In User Service)协议最初是由 Livingston 公司提出的，目的是为拨号用户进行认证和计费。后来经过多次改进，形成了一项通用的认证计费协议。

RADIUS 是一种客户机/服务器(C/S)结构，它的客户端最初就是 NAS(Net Access Server)服务器，现在任何运行 RADIUS 客户端软件的计算机都可以成为 RADIUS 的客户端。RADIUS 协议认证机制灵活，可以采用 PAP、CHAP 或者 UNIX 登录认证等多种方式。

RADIUS 的基本工作原理是用户接入 NZS，NAS 向 RADIUS 服务器使用 Access-Require 数据包提交用户信息，包括用户名、密码等相关信息，其中用户密码是经过 MD5 加密的，双方使用共享密钥，这个密钥不经过网络传播；RADIUS 服务器对用户名和密码的合法性进行检验，也可以对 NAS 进行类似的认证；如果合法，则向 NAS 返回 Access-Accept 数据包，允许用户进行下一步工作，否则返回 Access-Reject 数据包，拒绝用户访问；如果允许访问，NAS 向 RADIUS 服务器提出计费请求 Account-Require，RADIUS 服务器响应 Account-Accept，对用户的计费开始，同时用户可以进行自己的相关操作。

RADIUS 服务器和 NAS 服务器通过 UDP 协议进行通信，RADIUS 服务器的 1812 端口负责认证，1813 端口负责计费。采用 UDP 的基本考虑是因为 NAS 和 RADIUS 服务器大多在同一个局域网中，使用 UDP 更加快捷、方便。

RADIUS 协议还规定了重传机制。如果 NAS 向某个 RADIUS 服务器提交请求没有收到返回信息，那么可以要求备份 RADIUS 服务器重传。由于有多个备份 RADIUS 服务器，因此 NAS 进行重传的时候，可以采用轮询的方法。如果备份 RADIUS 服务器的密钥和以前 RADIUS 服务器的密钥不同，则需要重新进行认证。

RADIUS 协议应用范围很广，包括普通电话、上网业务计费，对 VPN 的支持可以使不同的拨入服务器的用户具有不同的权限。

2. 基于 DCE/Kerberos 的认证机制

DCE/Kerberos 是一种被证明非常安全的双向身份认证技术。该认证方法强调客户机对服务器的认证；而其他产品只解决了服务器对客户机的认证。

DCE/Kerberos 的身份认证的形式化过程如下。

1)　元素说明

- K——密钥。
- A——身份认证服务器。
- C——用户。
- P——访问授权服务器。
- PAC——访问授权服务器签发的授权凭证。
- S——应用服务器，如 Web 服务器、数据库服务器等。
- {…}K_n——用 K_n 加密大括号中的内容。

2)　实现步骤

(1)　用户 C 从身份认证服务器 A 获得通信凭证{K_1，C}K_a，该凭证可以理解为由身份认证服务器签发的一次性电子身份证或电子护照。

C->A: C （明文传输 C 的名字）
C<-A: {K_1，{K_1，C}K_a}K_c

(2)　用户 C 使用第一步得到的凭证{K_1，C}K_a，申请访问授权服务器 P 的通信凭证{K_2，C}K_p，该凭证可以理解为身份认证服务器为用户签发了访问授权服务器的电子介绍信。

C->A:{K_1，C}K_a，　{C，　MD-5 Checksum，　timestamp}K_1
C<-A:{K_2，{K_2，C}K_p}K_1

(3)　用户向授权服务器 P 申请授权凭证 PAC。授权服务器根据身份认证服务器签发的电子介绍信，为该用户签发一次性的出境许可。

C->P: {K_2，C}K_p，　{C，　MD-5 Checksum，　timestamp} K_2
C<-P: {K_3，　{PAC，　K_3}K_a}K_2

(4)　用户申请能够向服务器 S 证实自己身份，并得到授权许可的凭证{PAC，K_4}K_s，该凭证可以理解为应用服务器为该用户签发了一次性的入境签证。

C->A: {K_3，　{PAC，　K_3}K_a}K_1，　{C，　MD5 Checksum，　Timestamp}K_3




```
C<-A: {K4, {PAC, K4}K5}K3
```

(5) 用户 C 获得与应用服务器 S 通信的密钥 K_5，该密钥可以理解为应用服务器为用户签发了一次性的境内通行证。

```
C->S: {PAC, K4}K5, {C, MD-5 Checksum, Timestamp} K4
C<-S: {K5, Timestamp} K4
```

2.5　数字证书应用实例

数字证书主要应用于各种需要身份认证的场合，目前除广泛应用于网上银行、网上交易等商务应用外，数字证书还可以应用于发送安全电子邮件、加密文件等方面。

2.5.1　获得及安装免费数字证书

获得免费数字证书的方法很多，目前国内有很多 CA 中心提供试用型数字证书，其申请过程在网上即时完成，并可以免费使用。下面提供一个比较好的站点，申请地址为 http://www.itrus.com.cn/。

【例 2.1】 获得免费数字证书的方法。

(1) 登录后，单击【证书申请】按钮，选择【试用型个人数字证书申请】，注意只有安装了根证书(证书链)的计算机，才能完成后面的申请步骤，正常用户在 CA 中心申请数字证书。

(2) 按照提示，通过地址 http://www.itrus.com.cn/选择【安装试用 CA 证书链】。

(3) 安装成功出现提示框后，可以看到一个用户注册表单。按照表单上的提示，输入完整的个人资料进行用户注册。

(4) 用户注册成功后登录，选择使用安全证书，出现注册国际安全电子邮件证书的表单，依照提示填写、提交，进行上述步骤后，系统将发送一封申请成功的信件到读者申请时使用的邮箱内，其中包括业务受理号、密码、数字证书下载的地址。

(5) 单击数字证书下载地址，填写业务受理号和密码。提交后，可以看到“祝贺你！你的数字证书已经成功产生并安装”的信息，表明用户的证书已经成功安装。

2.5.2　在 IE 中查看数字证书

微软的浏览器自带一个数字证书管理器，通过这个管理器可以查看数字证书。

【例 2.2】 通过 IE 查看数字证书。

(1) 首先在打开的 Internet Explorer 中，选择【工具】|【Internet 选项】命令。在弹出的对话框中选择【内容】选项卡，单击【证书】按钮来查看读者信任的当前证书的列表。

(2) 切换到【个人】选项卡可以查看已经申请的个人数字证书，下面是申请的免费数字证书，如图 2.17 所示。

(3) 选择要查看的个人数字证书，然后单击【查看】按钮，可以查看证书的详细信息。图 2.18 是一个数字证书的详细信息列表。

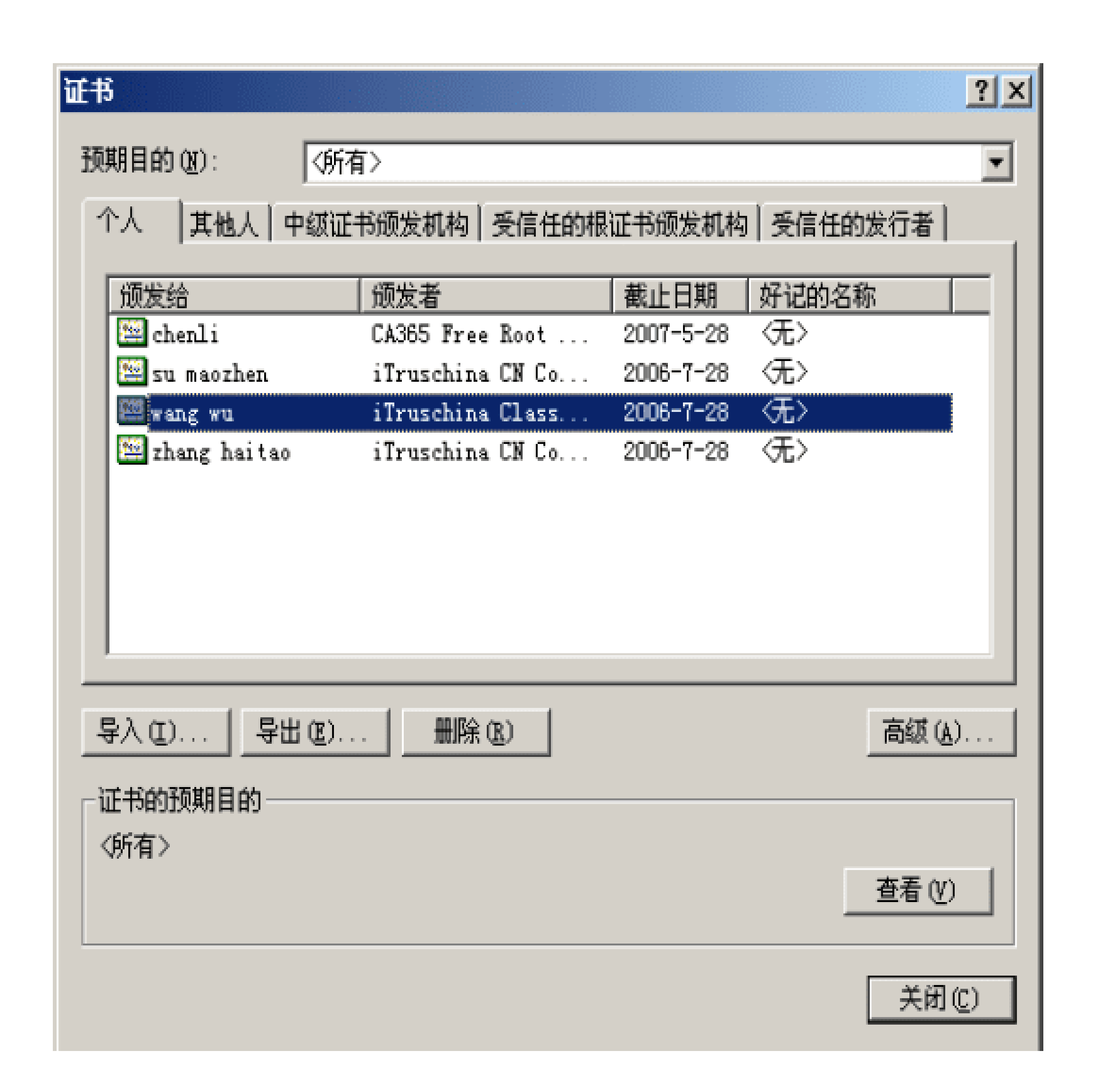


图 2.17　免费数字证书

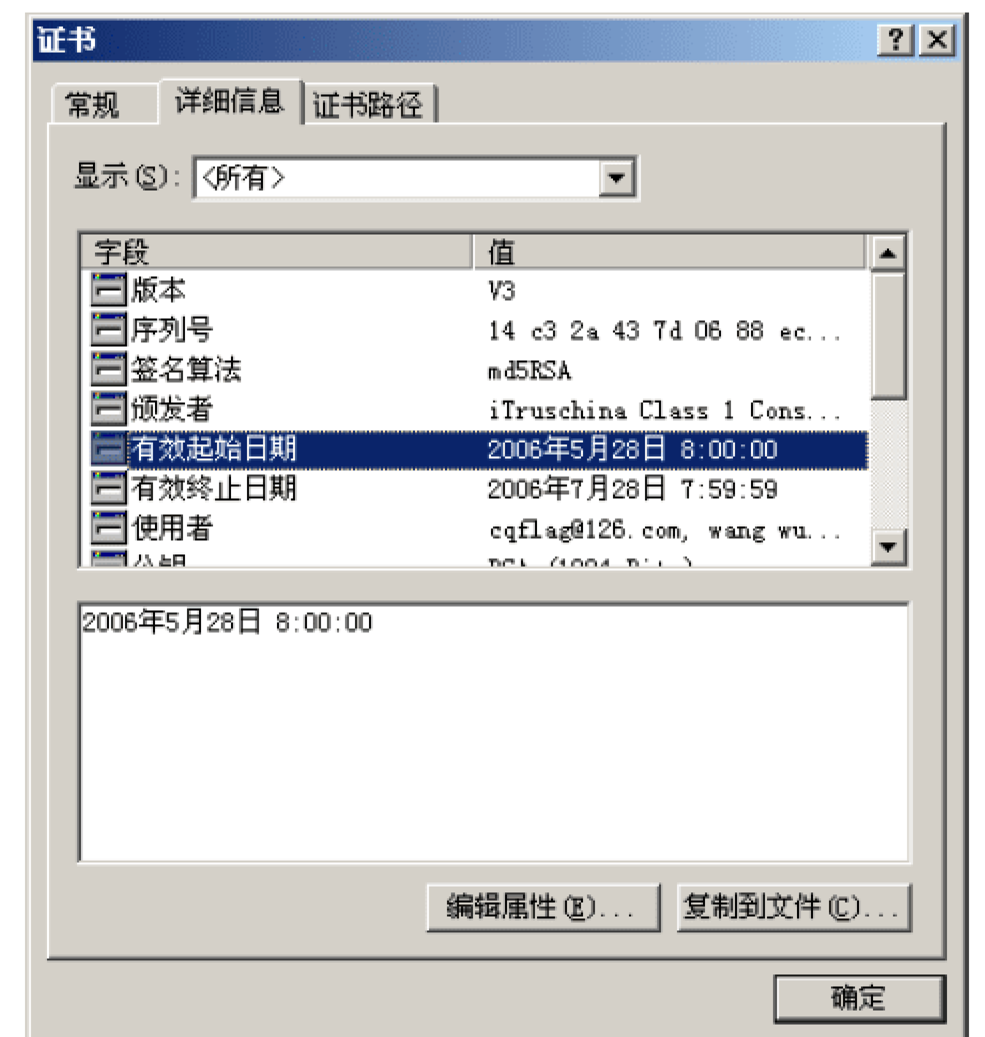


图 2.18　数字证书的详细信息列表

下面是在数字证书中所包含的常见元素。

- 版本：用来区别 X.509 的各种连续的版本。
- 序列号：序列号是一个整数值，在发行的证书颁发机构中是唯一的。序列号与证书有明确联系，就像身份证号码和公民日常登记有明确联系一样。
- 签名算法：用于识别证书颁发机构签署证书的算法。证书颁发机构使用它的私钥对每个证书进行签名。
- 颁发者：颁发者是创建这个证书的机构。
- 有效起始日期和有效终止日期：证书有效的起止日期，类似于信用卡的期限。
- 使用者：证书进行身份验证的主体对象。
- 公钥：为证书识别的主体提供公钥和签名算法。
- 签名：证书签名覆盖了证书的所有其他字段。签名是其他字段的 Hash 代码，使用证书颁发机构的私钥进行加密，保证整个证书中信息的完整性。如果有人使用了证书颁发机构的公钥来解密这个 Hash 代码，同时计算了证书的 Hash 代码，而两者并不相同，那么证书的某一部分就肯定被非法篡改了。

有了数字证书以后，可以发送加密和签名电子邮件，还可以应用于公众网络上的商务活动和行政活动，应用范围涉及需要身份认证及数据安全的各个行业，如访问安全站点、网上招标投标、网上签约、网上订购、安全网上公文传送、网上办公、网上缴费、网上缴税、网上购物等网上的安全电子事务处理和安全电子交易活动等。随着电子商务和电子政务的不断发展，数字证书的颁发机构 CA 中心将作为一种基础设施为电子商务的发展提供可靠的保障。所以，网络发展得越快，人们对网络安全的要求也就越高，了解数字证书并学会一些数字证书的操作将有利于更加安全地在网上冲浪。

2.5.3　发送安全邮件

数字证书最常见的应用就是发送安全邮件，即利用安全邮件数字证书对电子邮件签名



和加密，这样既能保证发送的签名邮件不会被篡改，又使外人无法阅读加密邮件的内容。下面以 Outlook 2000 为例介绍安全发送邮件的方法。

1. 邮件账号与数字证书绑定

【例 2.3】 将邮件账号与数字证书绑定。

(1) 启动 Outlook 2000，选择【工具】|【选项】命令，在弹出的对话框中选择【安全】选项卡，单击【设置安全电子邮件】按钮，打开【更改安全性设置】对话框，如图 2.19 所示。

(2) 输入安全设置名称 safe1，选中【该安全邮件格式的默认安全性设置】复选框，单击【选择】按钮为账户绑定一个数字证书。

(3) 单击【确定】按钮退出。以后发送数字签名邮件时，将使用该证书进行签名。

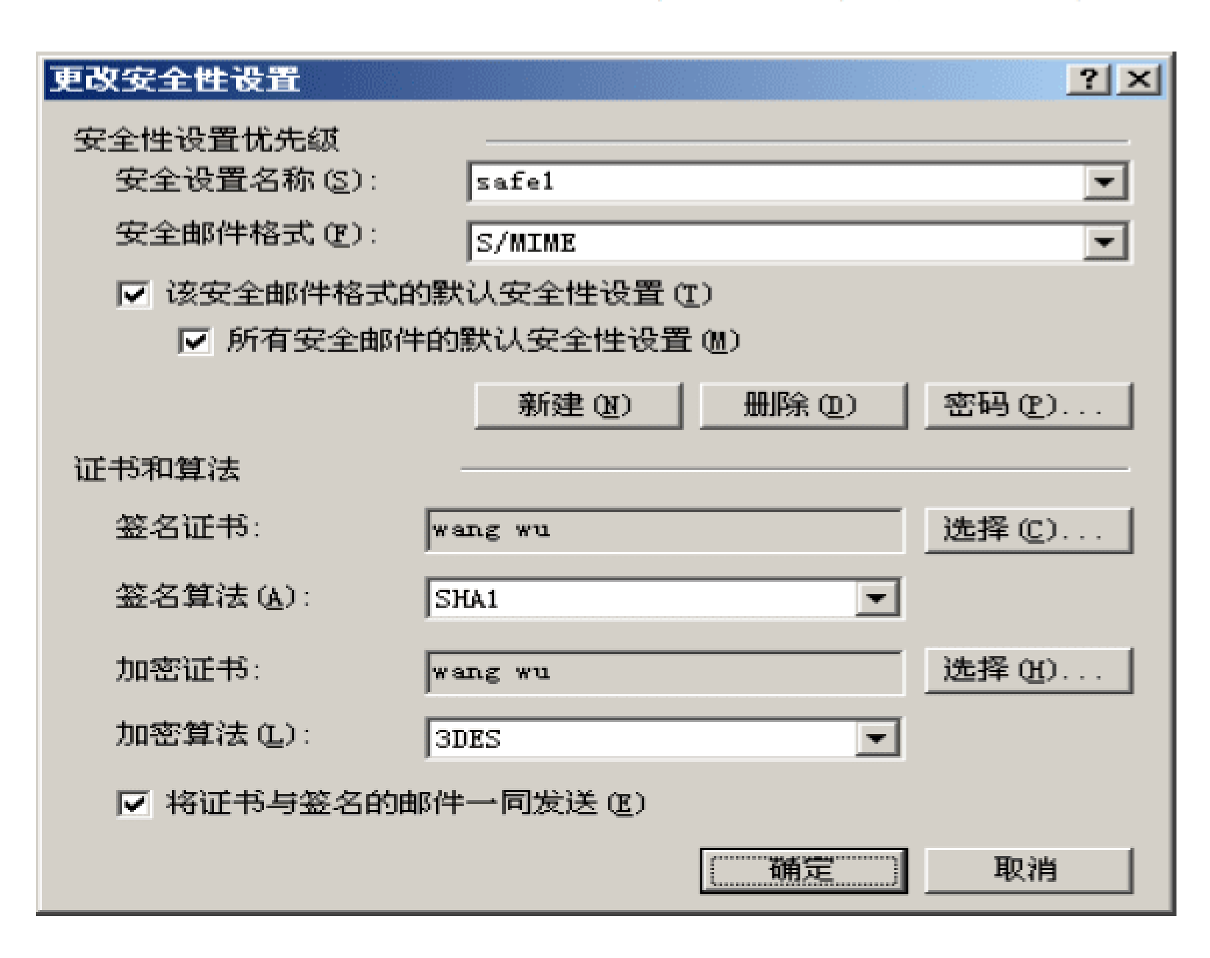


图 2.19 更改安全设置

2. 发送带数字签名的邮件

【例 2.4】 发送带数字签名的邮件。

(1) 启动 Outlook 2000，单击工具栏中的【新建】按钮进入写邮件窗口，开始撰写一封新邮件。填上发件人、收件人、标题，写好信。

(2) 单击工具栏上的【选项】按钮，打开【邮件选项】对话框，如图 2.20 所示，选中【给待发邮件添加数字签名】复选框。

(3) 单击【发送】按钮即可。

当对方收到并打开该邮件时，将看到【数字签名邮件】的提示信息，在邮件内容窗口的右边，有个红色的【数字签名】图标，单击该图标就可看到数字签名信息，由此便可确认该邮件是谁发出的并且中途没有被篡改过。

3. 发送加密邮件

必须首先获得对方的公钥，然后才能给他发加密邮件。

1) 获得对方公钥的方法

可以让收件人先发送一份签名邮件来获取对方的公钥，或者直接到对方注册的安全认证中心的网站上查询并下载对方的公钥。

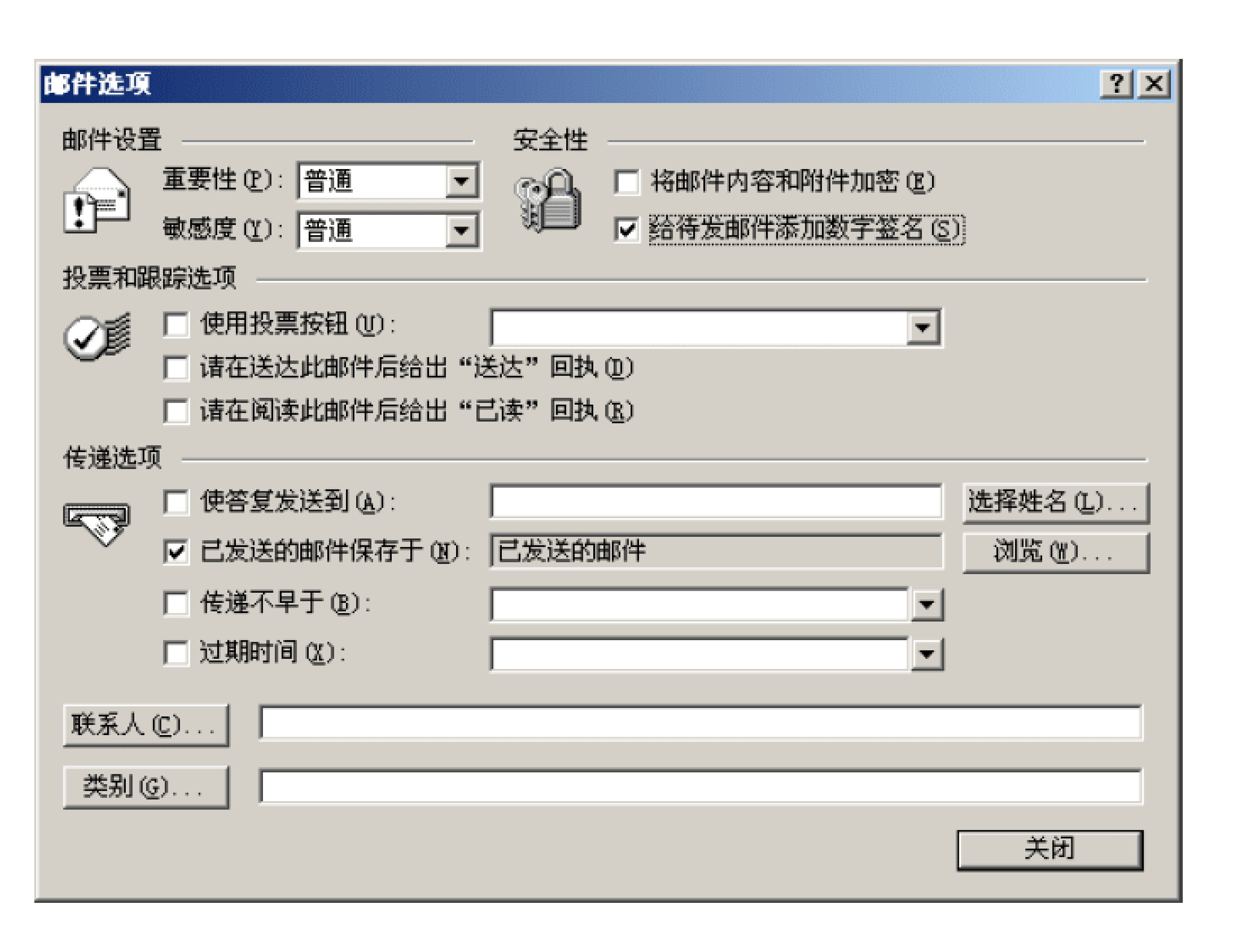


图 2.20　为邮件添加数字签名

2)　创建邮件并发送

加密邮件的发送方法，与以上发送签名邮件的方法类似，不过当单击【安全设置】按钮时，在【安全属性】窗口中要选中【加密邮件内容和附件】复选框。

【例 2.5】 备份你的证书及私钥。

(1)　打开 IE 窗口，选择【工具】|【Internet 选项】命令，打开【Internet 选项】对话框，切换到【内容】选项卡，单击【证书】按钮。

(2)　在弹出的【证书】对话框中选择需要备份的证书，单击【导出】按钮，如图 2.21 所示。

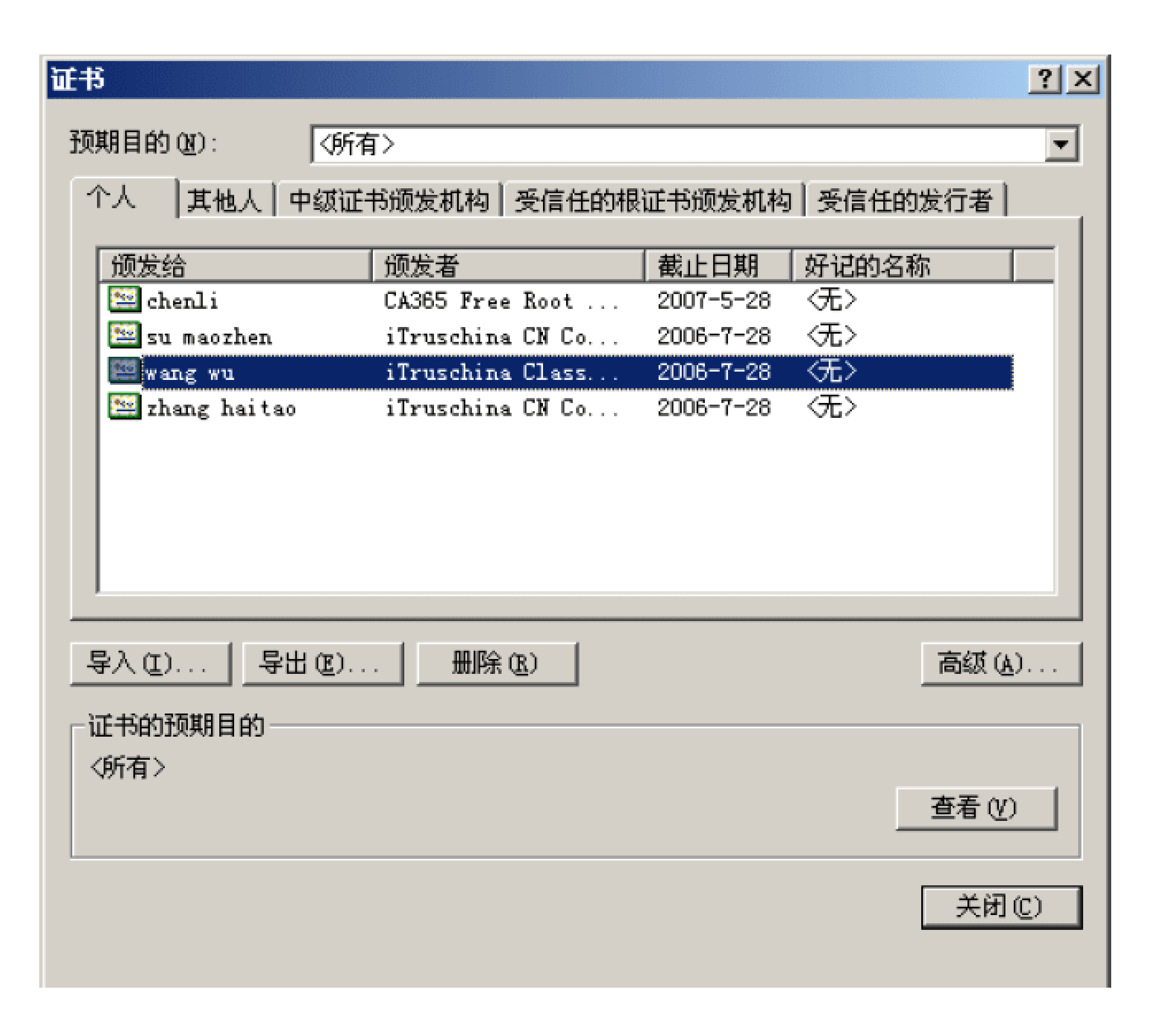


图 2.21　导出证书

(3)　进入【证书导出向导】对话框，单击【下一步】按钮，如图 2.22 所示。

(4)　如果想要保存自己的私钥信息，请选中【是，导出私钥】单选按钮，如图 2.23 所示。





图 2.22　证书导出向导第一步

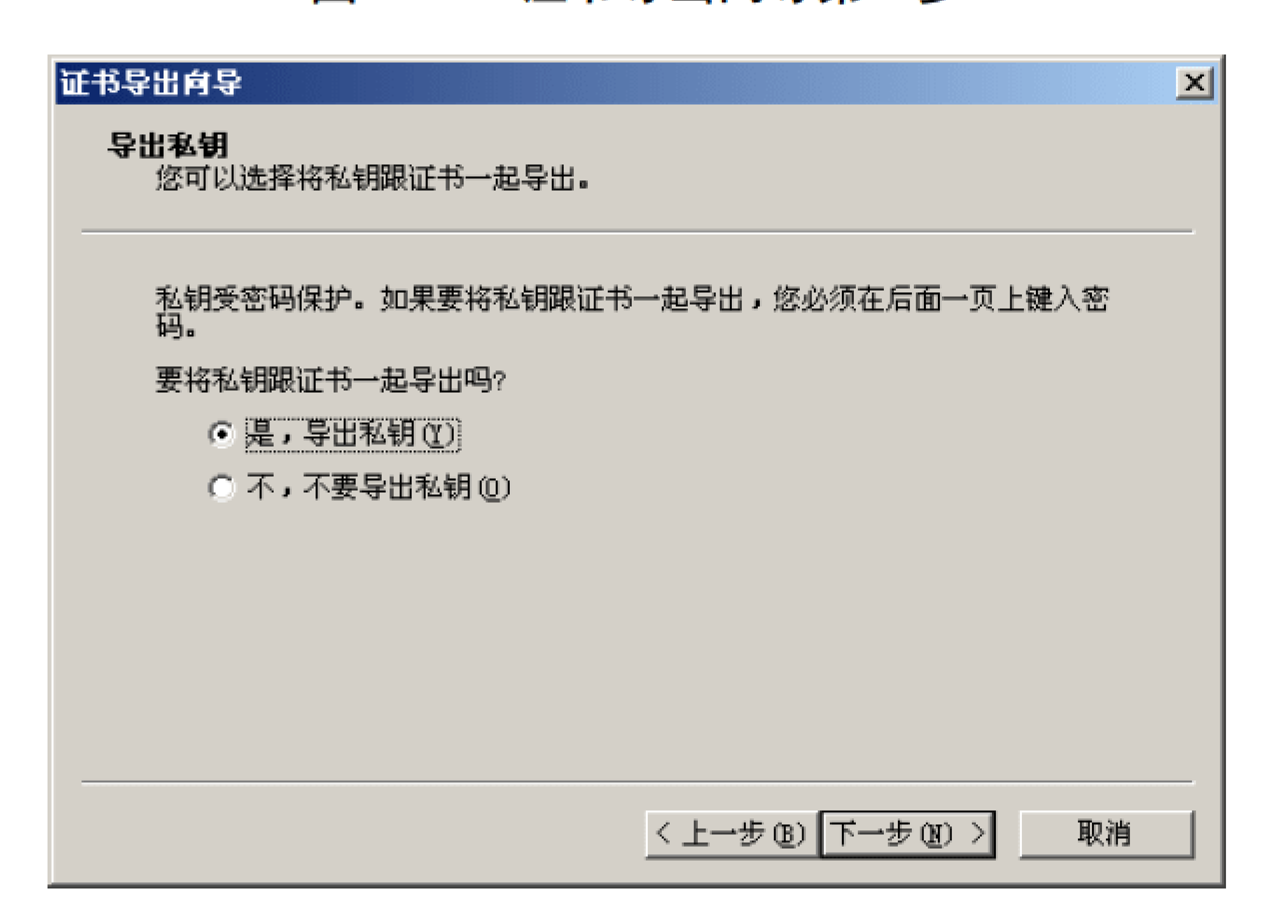


图 2.23　证书导出向导第二步——导出私钥

(5)　单击【下一步】按钮，选择导出文件的格式，如图 2.24 所示。

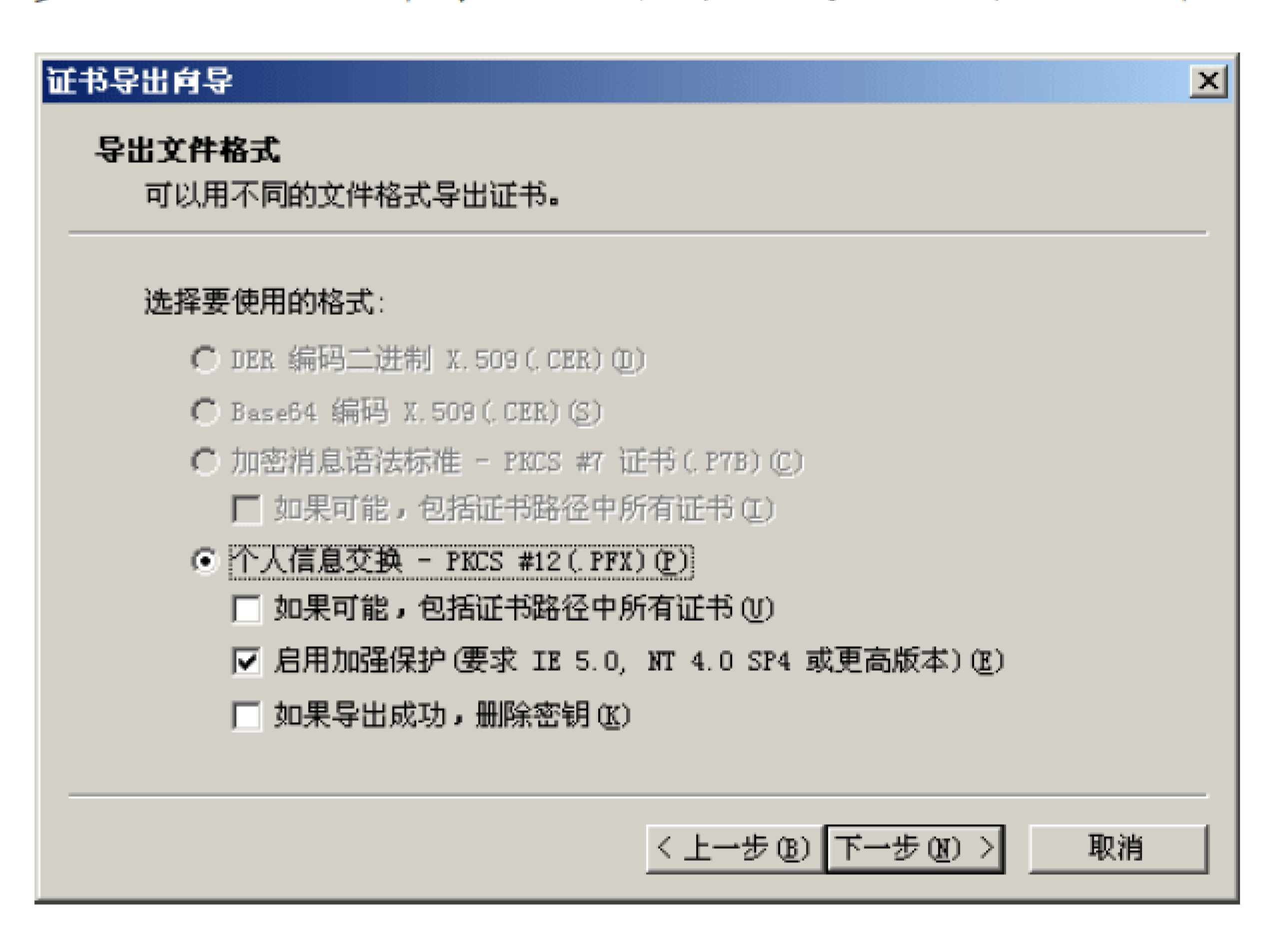


图 2.24　证书导出向导第三步——选择导出文件的格式

(6)　单击【下一步】按钮，设置私钥保护密码，谨慎保护此密码，只用拥有此密码才可以使用导出的私钥文件，如图 2.25 所示。

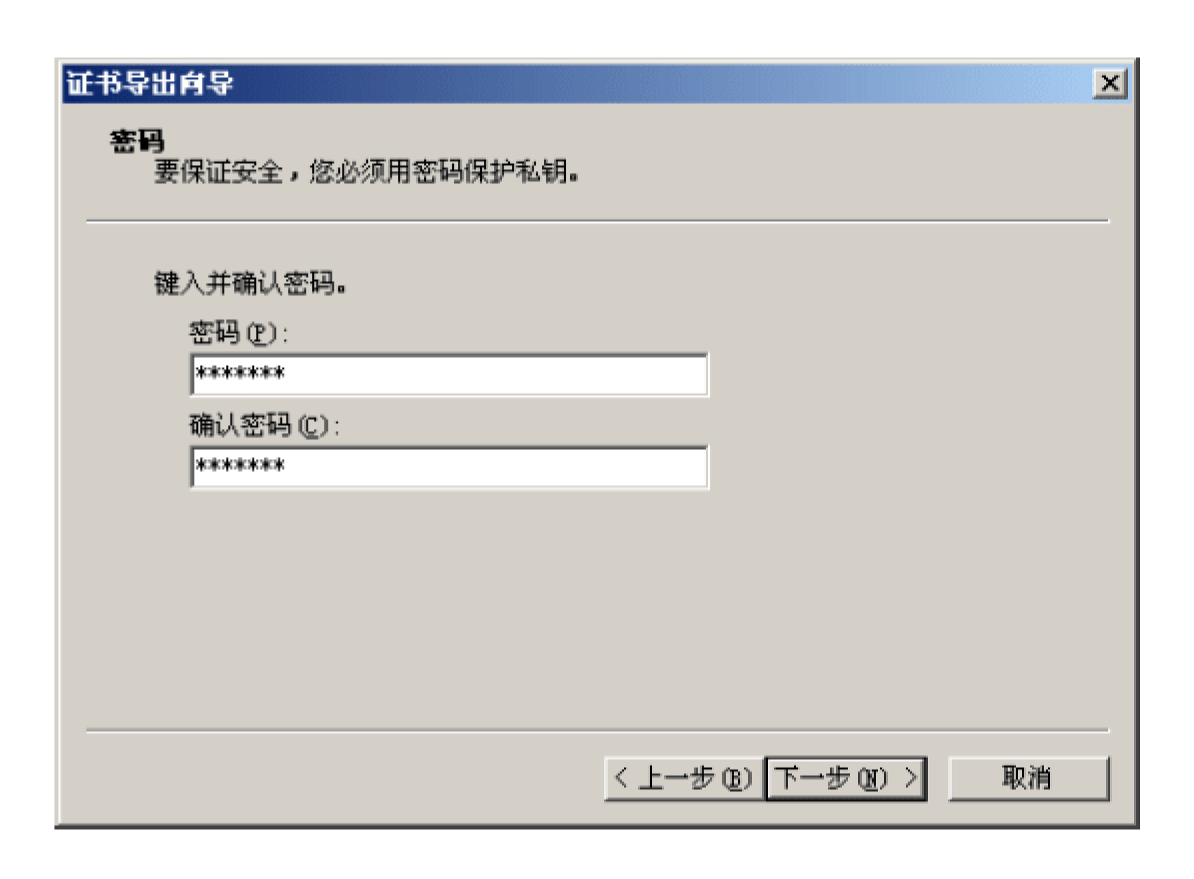


图 2.25　导出证书向导第四步——设置私钥保护密码

(7)　单击【下一步】按钮，指定导出文件名及存放路径，单击【下一步】按钮。建议将私钥备份到可移动的存储设备中，如 U 盘等，如图 2.26 所示。

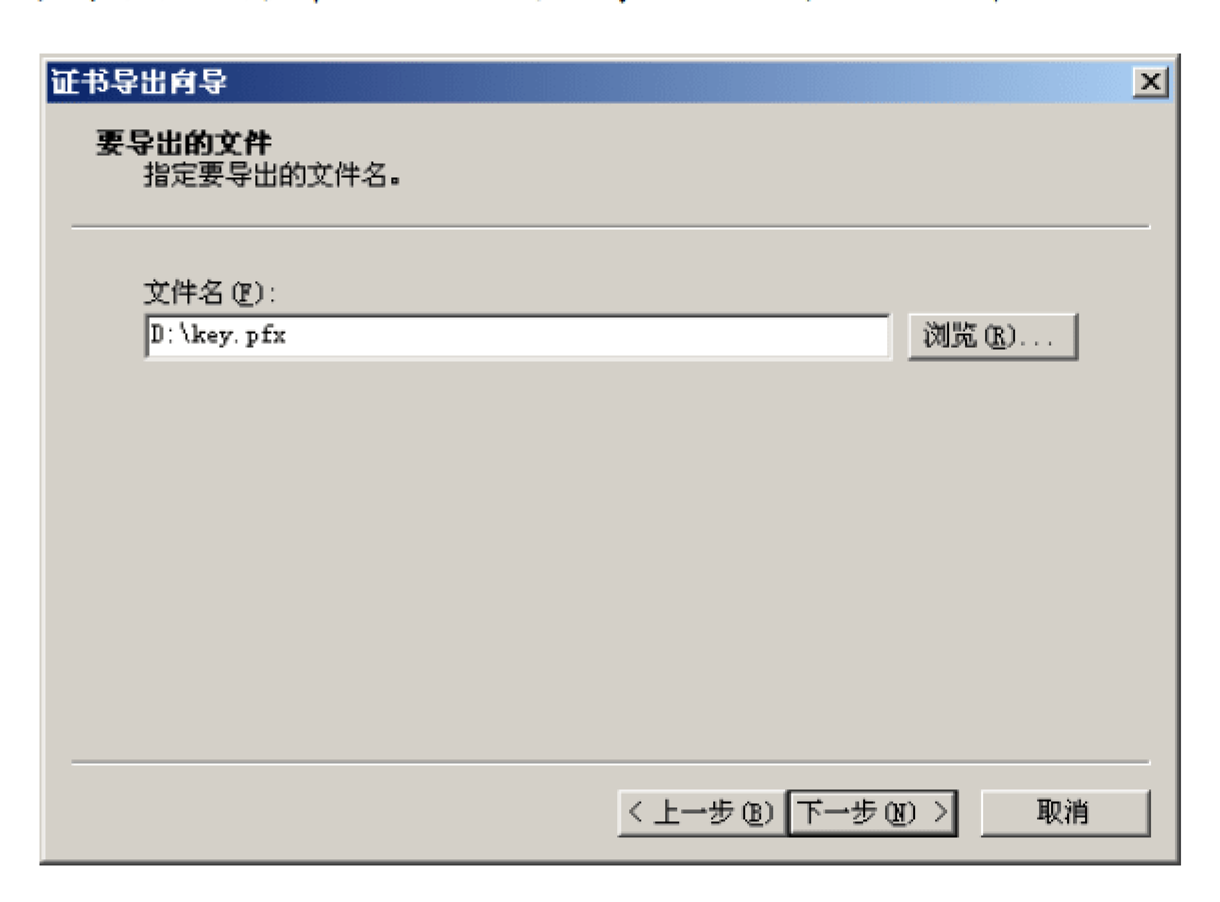


图 2.26　导出证书向导第五步——指定导出文件名

(8)　单击【完成】按钮，如图 2.27 所示。

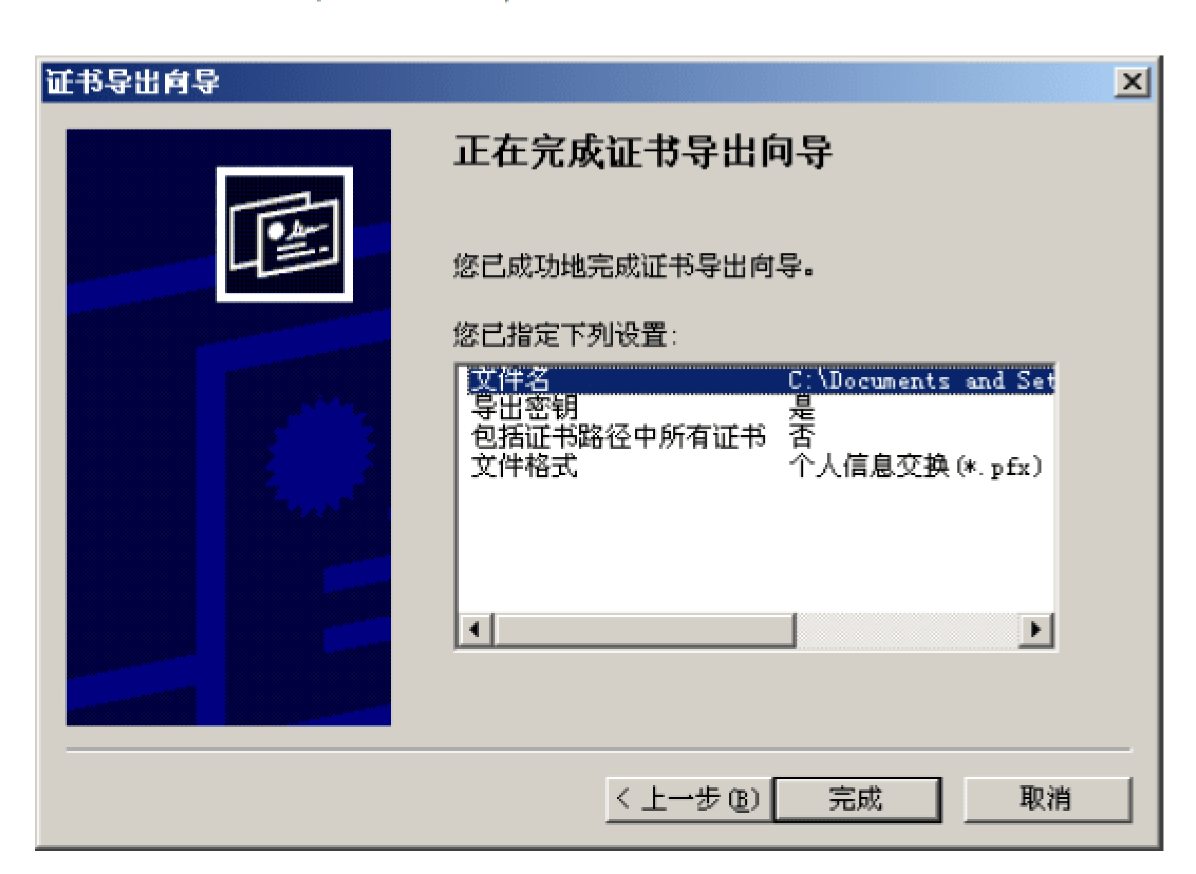
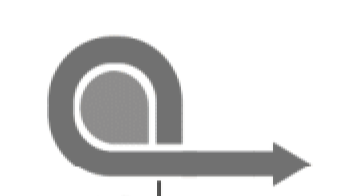


图 2.27　导出证书向导第六步——完成

【例 2.6】　证书和私钥的恢复。

(1)　打开 IE 窗口，选择【工具】|【Internet 选项】命令，打开【Internet 选项】对话框，



选择【内容】选项卡，单击【证书】按钮。

(2) 单击【导入】按钮，进入证书导入界面，如图 2.28 所示。



图 2.28　证书导入界面

(3) 选择需要导入证书的存放路径，如图 2.29 所示。



图 2.29　选择证书的存放路径

(4) 输入密钥的保护密码，如图 2.30 所示。

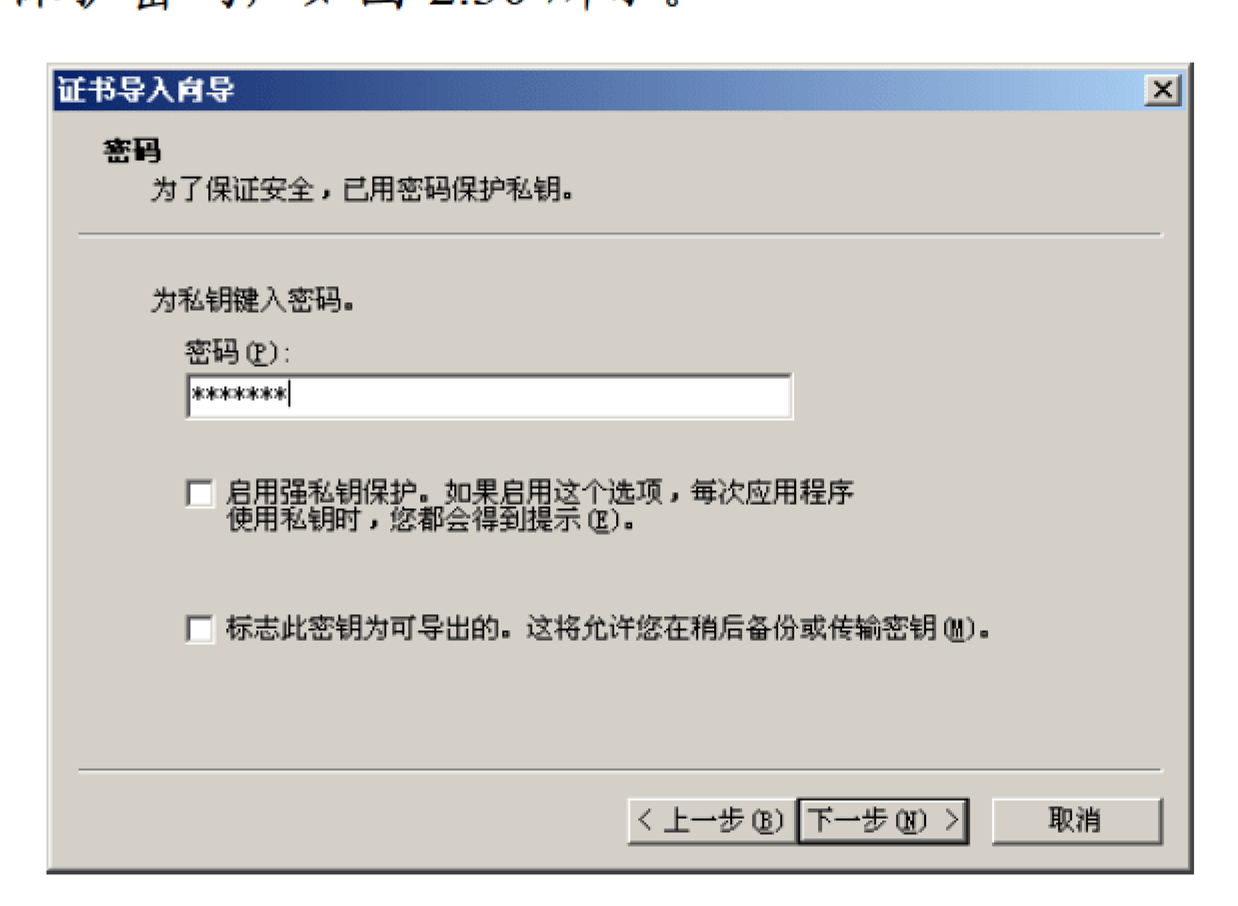


图 2.30　输入密钥的保护密码

(5) 指定证书的存放位置，如图 2.31 所示。

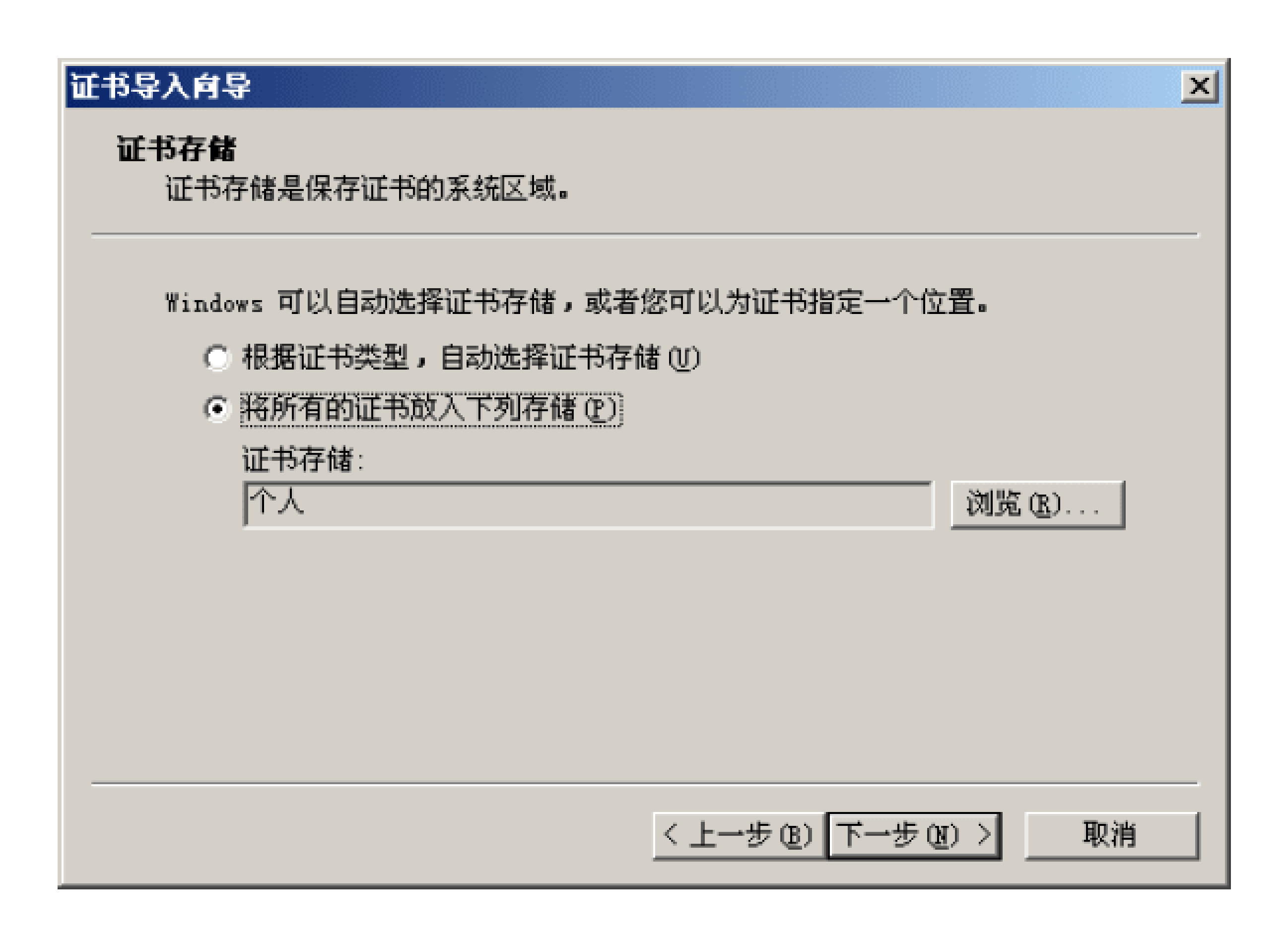


图 2.31 指定证书的存放位置

(6) 单击【完成】按钮，结束密钥的导入，如图 2.32 所示。

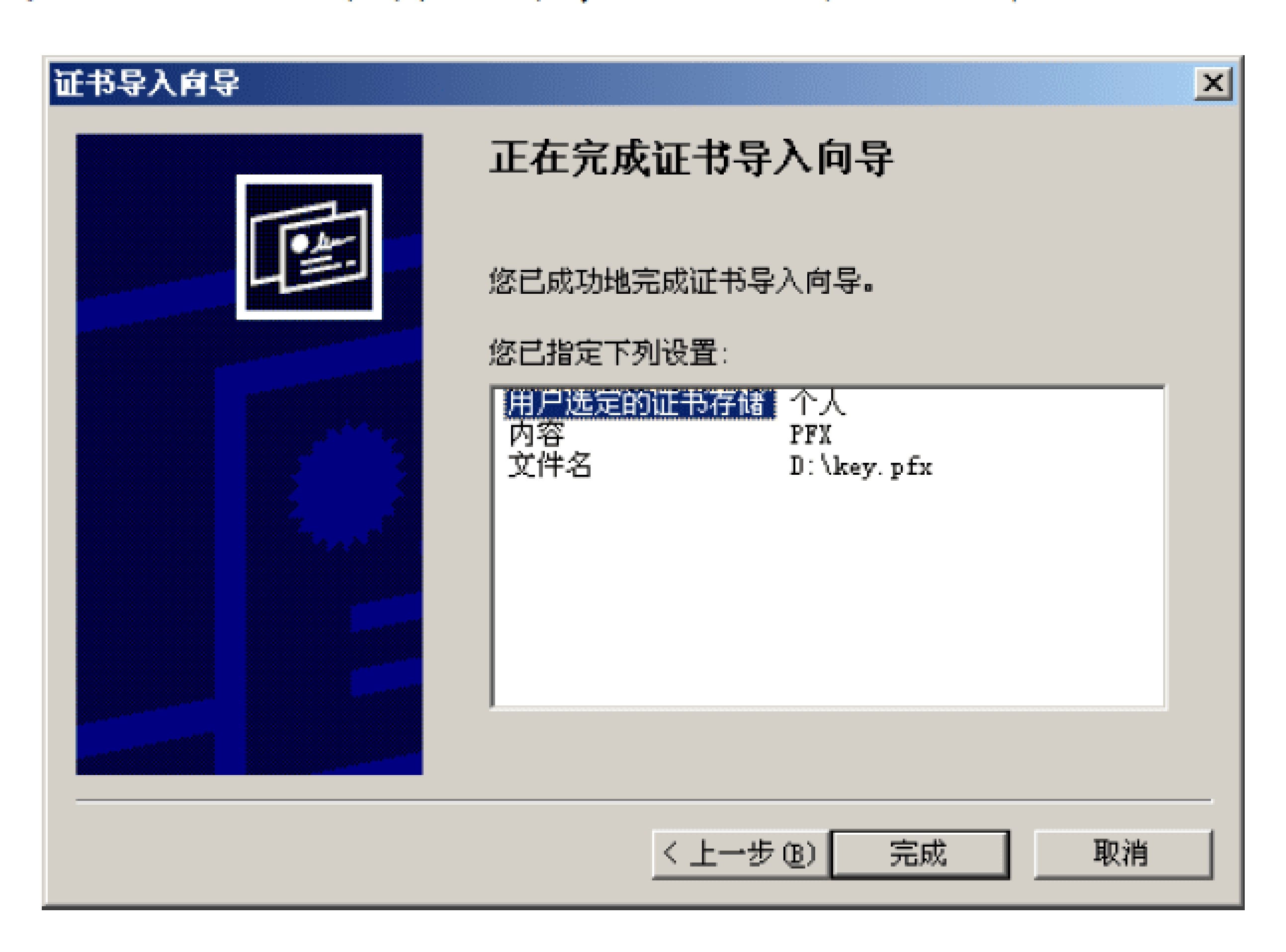


图 2.32 结束密钥的导入

2.5.4 检查 Windows 是否为微软正版

如果想知道自己的 Windows 是否为微软正版软件，只要验证其核心文件是否被替换过即可，那么如何知道核心文件是否替换过呢？可以使用工具来检查这些文件的数字签名，Windows 2000/ XP /中有“文件签名验证”工具，Windows 9X 则提供了“系统文件检查器”，使用这些工具可以知道系统文件的数字签名状态，假如它们都经过了数字签名，则说明 Windows 未被篡改过、是微软原版的，下面以 Windows Server 2003 为例介绍验证的方法。

【例 2.7】 检查 Windows 是否为微软正版。

(1) 选择【开始】|【运行】命令，打开【运行】对话框，输入 sigverif，打开【文件签名验证】对话框。

(2) 单击【开始】按钮检查每个系统文件的数字签名，过一会儿将打开一个对话框，如图 2.33 所示，列出所有未经过数字签名的文件，如果发现列表中有 winlogon.exe、licdll.dll 这两个文件，那么 Windows 就被篡改过了，否则即为微软正版的。



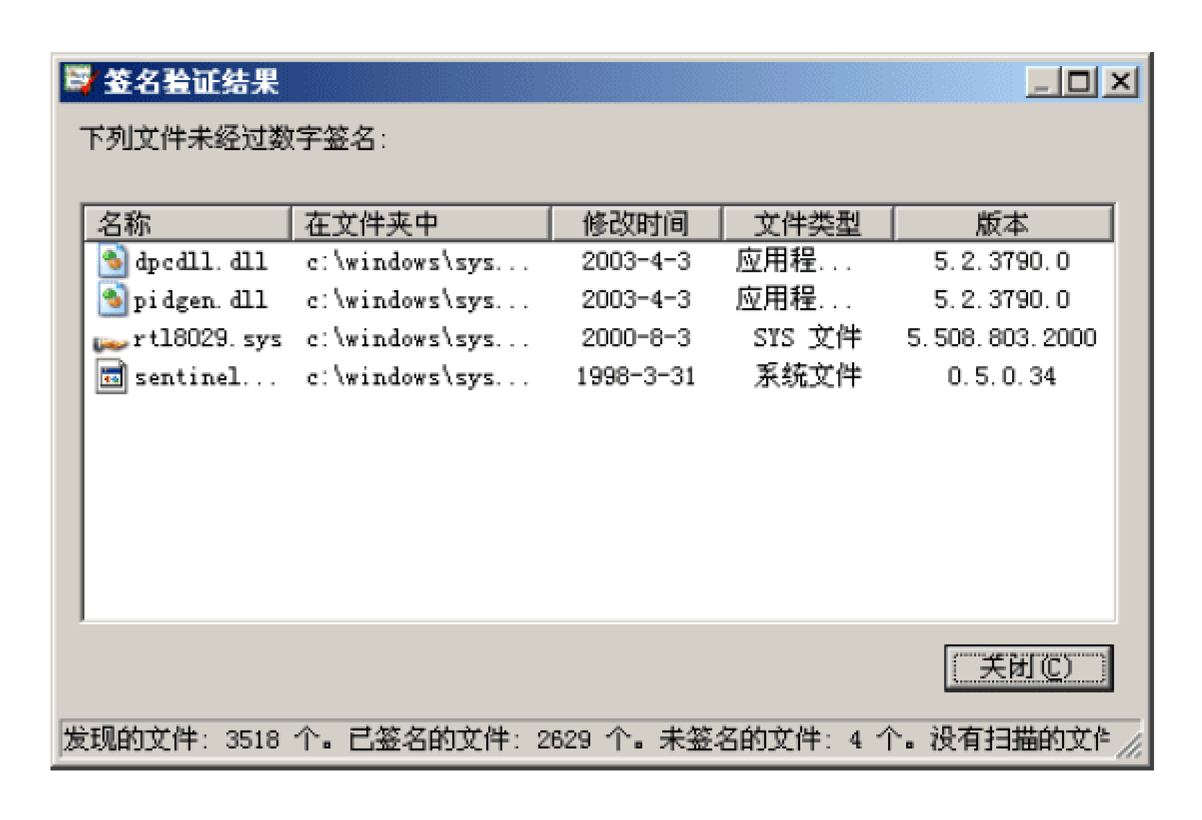


图 2.33　签名验证结果

复习思考题二

一、填空题

1. 需要隐藏的消息叫作________。明文被变换成另一种隐藏形式被称为________。这种变换叫作________。

2. 加密算法和解密算法通常是在________控制下进行的，加密算法所采用的密钥称为________，解密算法所使用的密钥叫作________。

3. 传统的加密方法可以分成替代密码与______换位密码两类。

4. 密钥长度一般是以________为单位，也有以______为单位的，密钥的长度对密钥的有直接的影响。

5. 密钥保护技术涉及密钥的________、________、________、使用、更换、销毁等多个方面。

6. 数字证书通常分为________、________和软件证书。

7. 数字时间戳服务是网上电子商务安全服务项目之一，能提供________的日期和时间信息的安全保护。

8. 认证技术一般可以分为________和________两种。

9. 认证技术主要解决网络通信过程中通信双方________的认可。

二、选择题

1. 为了确定信息在网络传输过程中是否被他人篡改，一般采用的技术是(　　)。

A. 防火墙技术　　B. 数据库技术　　C. 消息认证技术　　D. 文件交换技术

2. KDC 分发密钥时，进行通信的两台主机都需要向 KDC 申请会话密钥。主机与 KDC 通信时使用的是(　　)。

A. 会话密钥　　B. 公开密钥　　C. 二者共享的永久密钥　　D. 临时密钥

3. 用户 A 从 CA 得到了用户 B 的数字证书，用户 A 可以从该数字证书中得到用户 B 的(　　)。

A. 私钥　　B. 数字签名　　C. 口令　　D. 公钥

4. 计算机网络系统中广泛使用的 DES 算法属于(　　)。

A. 不对称加密 B. 对称加密 C. 不可逆加密 D. 公开密钥加密

5. 在公钥密码体制中，用于加密的密钥为(　　)。

A. 公钥 B. 私钥 C. 公钥与私钥 D. 公钥或私钥

6. PKI 是指(　　)

A. 公共密钥基础结构 B. Public Key Infrastructure C. 上述都对

7. 证书颁发机构 CA 的功能包括(　　)。

A. 颁发证书 B. 吊销证书

C. 发布证书吊销列表 CRL D. 上述都对

8. 在 Windows 中，可以为下列(　　)组件申请证书。

A. 计算机 B. 服务 C. 用户 D. 上述都对

三、简答题

1. 简述密码学的概念。
2. 简述加密、解密的过程。
3. 什么是对称密钥加密？
4. 什么是公开密钥加密？
5. 数字签名有哪几种实现方法？
6. 数字时间戳的用途是什么？
7. 简述报文摘要技术的实现过程。
8. 简述基于 3 种基本途径的身份认证技术的特点及用途。
9. 信息认证技术的用途是什么？
10. 如何发送安全的电子邮件？

第 3 章　操作系统安全技术

学习目标

网络操作系统是用于管理计算机网络中的各种软、硬件资源，实现资源共享，并为整个网络中的用户提供服务，保证网络系统正常运行的一种系统软件。如何确保网络操作系统的安全，是网络安全的根本所在，只有网络操作系统安全、可靠，才能保证整个网络的安全。因此，详细分析系统的安全机制，找出它可能存在的安全隐患，给出相应的安全策略和保护措施是十分必要的。本章主要系统学习：操作系统漏洞的概念；Windows 操作系统中的漏洞及其解决方法；Linux 操作系统中的漏洞及其解决方法。通过本章的学习，读者应掌握以下内容：

- 掌握漏洞的概念及其对操作系统的影响；Windows 操作系统中的漏洞及其解决方法。
- 了解 Linux 操作系统中的漏洞及其解决方法。

3.1　操作系统的漏洞

一般来说，计算机网络系统的安全威胁主要来自黑客攻击和计算机病毒两个方面。那么黑客攻击为什么能够经常得逞呢?主要原因是很多人，尤其是很多网络管理员没有起码的网络安全防范意识，未能针对所用的网络操作系统采取有效的安全策略和安全机制，从而给黑客以可乘之机。因此要更好地保证网络安全，第一步就是确保操作系统的安全。

操作系统的选择是关键的一步，根据用户的要求不同，选择也有所不同，整体上可以分为两种类型：第一种是选用 Windows 2000、Windows XP 或者 Windows Server 2003 的用户，第二种是使用 Linux 操作系统的用户。

从安全的角度来说，各种操作系统不可能百分之百的无缺陷、无漏洞。另外，编程人员为自己使用方便而在软件中留有“后门”，一旦“漏洞”及“后门”为外人所知，就会成为整个网络系统受攻击的首选目标和薄弱环节。据调查显示，网络安全的威胁大多数情况下仍来自于黑客和病毒专家对操作系统漏洞的利用。

3.1.1　系统漏洞的概念

在计算机网络安全领域中，“漏洞”是指硬件、软件或策略上的缺陷，这种缺陷导致非法用户未经授权而获得访问系统的权限或增加其访问权限。有了这种访问权限，非法用户就可以为所欲为，从而造成对网络安全的威胁。其实，每个平台无论是硬件还是软件都存在漏洞。漏洞与后门是不同的，漏洞是难以预知的，后门则是人为故意设置的。后门是软、硬件制造者为了进行非授权访问而在程序中故意设置的万能访问口令，这些口令无论是被攻破，还是只掌握在制造者手中，都对使用者的系统安全构成了严重的威胁。

系统漏洞又称安全缺陷，是某个程序(包括操作系统)在设计时未考虑周全，当程序遇

到一个看似合理，但实际无法处理的问题时，引发的不可预见的错误。系统漏洞对用户造成的不良后果如下。

漏洞被恶意用户利用，会造成信息泄露，如黑客攻击网站就是利用网络服务器操作系统的漏洞。对用户操作造成不便，如不明原因的死机和丢失文件等。只有堵住系统漏洞，用户才会有一个安全和稳定的工作环境。

系统漏洞的产生原因大致有 3 个。

(1) 在程序编写过程中，编程人员为了达到不可告人的目的，有意地在程序的隐蔽处留下各种各样的后门，供日后使用。随着法律的完善，这类漏洞将越来越少(别有用心的除外)。

(2) 由于编程人员的水平问题，以及经验和当时安全技术加密方法所限，在程序中总会或多或少地存在不足之处，这些地方有的影响程序的效率，有的会导致非授权用户的权力加大提升。安全与不安全从来都是相对的。

(3) 由于硬件原因，使编程人员无法弥补其漏洞，从而使硬件的问题通过软件表现出来。

漏洞问题是与时间紧密相关的。一个系统从发布的那一天起，随着用户的深入使用，系统中存在的漏洞会被不断暴露出来，一些早先被发现的漏洞会不断被系统供应商发布的补丁软件修补，或在以后发布的新版系统中得以纠正。而在新版系统纠正了旧版本中具有漏洞的同时，也会引入一些新的漏洞和错误，因而随着时间的推移，旧的漏洞会不断消失，新的漏洞会不断出现，漏洞问题也就会长期存在。

脱离具体的时间和具体的系统环境来讨论漏洞问题是毫无意义的。要针对目标系统的操作系统版本及在其上运行的软件版本以及服务运行设置等实际环境来具体谈论其中可能存在的漏洞及其可行的解决办法。

同时，对漏洞问题的研究必须要跟踪当前最新的计算机系统及其安全问题的最新发展动态。这一点与对计算机病毒发展问题的研究相似。如果不能保持对新技术的跟踪，就没有谈论系统安全漏洞问题的发言权，以前所做的工作也会逐渐失去价值。

3.1.2 漏洞的类型

安全漏洞存在不同的类型，包括允许拒绝服务的漏洞、缓冲区溢出漏洞、允许有限权限的本地用户未经授权加大其权限的漏洞和允许外来团体(在远程主机上)未经授权访问网络的漏洞。

1. 允许拒绝服务的漏洞

允许拒绝服务的漏洞可能导致拒绝服务发生。“拒绝服务”是一种常见的恶作剧式的攻击方式，它使服务器忙于处理一些繁杂的任务，从而消耗大量的处理时间，而无暇顾及用户的合法请求。

允许拒绝访问的漏洞属于 C 类，是不太严重的漏洞。对于大规模的网络或站点，拒绝服务及其攻击造成的影响是有限的；然而对于小规模的站点，可能会遭到拒绝服务导致的重创，特别是对于站点只是一台单独的计算机更是如此。这类漏洞存在于操作系统网络传送本身，是操作系统软件本身存在的漏洞。当存在这种漏洞时，必须通过软件开发者或销



售商的弥补予以纠正。

拒绝服务攻击是一个人或多个人利用 Internet 协议组的某些方面拒绝其他用户对系统或信息进行合法访问的攻击。在 TCPSYN 攻击中，大量连接请求传给服务器，导致其请求信息被淹没，致使服务器反应很慢或信息不能到达，从而使用户无法正常工作。

另外还有其他形式的拒绝服务的攻击，如某些拒绝服务攻击的实现可以针对个人而不是针对网络用户的这种类型的攻击不涉及任何漏洞，而是利用了 Web 的基本设计。

并不是每个拒绝服务攻击都需要在 Internet 上发起，拒绝服务攻击也可以在本地机甚至在没有网络环境的情况下发生。

2. 缓冲区溢出漏洞

当向数组中写入一个字符串，并且越过数组边界的时候，就会发生缓冲区溢出。下列缓冲区溢出的情况，可能会引起安全问题。

(1) 读操作直接输入到缓冲区。

(2) 从一个大的缓冲区复制到一个小的缓冲区。

(3) 对输入的缓冲区做其他的操作。

如果输入是可信的，则不会成为安全漏洞，但它也会成为潜在的安全隐患。这个问题在大部分的 UNIX 环境中很突出。如果数组是一些函数的局部变量，那么它的返回地址很有可能就在这些局部变量的堆栈中，这样就使得实现这种漏洞变得十分容易，在过去的几年中，有无数漏洞是由此造成的，有时甚至在其他地方的缓冲区都会产生安全漏洞，尤其是在函数指针附近的时候。

3. 允许有权限的本地用户未经授权增加其权限的漏洞

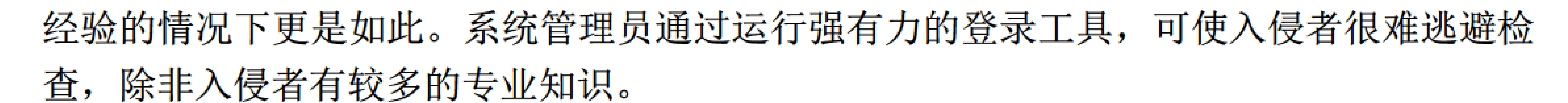
这是一种允许本地用户非法访问的漏洞，属 B 类。这类漏洞危险性很大，允许本地用户非法访问的漏洞所产生的影响是巨大的。例如，Sendmail 这类程序中的漏洞特别值得重视，因为网络上所有的用户都有使用这个程序的基本权限，否则用户将无法发送邮件。因此 Sendmail 中的任何漏洞都是十分危险的。

允许本地用户非法访问的漏洞一般在多种平台的应用程序中均有存在，它们由应用程序中的一些缺陷引起。有些常见的编程错误导致了这种漏洞的产生。

Sendmail 是 Linux 操作系统中发送电子邮件最盛行的方法，是 Internet 上 E-mail 系统的中心。这个程序一般在启动时初始化，并且只要机器可用它便可用。在其处于活动状态时，Sendmail(在端口 25)侦听网络空间上的发送和请求。因为只有 root 有权启动和维护 Sendmail 程序，所以当其他有相同权限的用户要启动 Sendmail 的时候，一般要检验用户的身份。然而由于一个代码错误，Sendmail 在例程模式下可以以一种绕过潜入的方式激活。当绕过检查后，任何本地用户都可以在例程下启动 Sendmail。另外，在 8.7 版本中，Sendmail 收到一个 Signup 信号时会重启，此时调用 exec(2)使 Sendmail 重新开始操作(非 root 启动的 Sendmail)；这次重新操作被系统认为是由 root 引发的，即这次调用使 Sendmail 具有了超级权限，所以入侵者利用这个漏洞非法获得了超级用户权限，继而对系统实施攻击。

权限有限的本地用户在未经授权的情况下，通过各种手段提高其访问权限。这种攻击对系统安全威胁很大。

管理员可以利用允许本地用户非法访问的漏洞来检查出入侵者，特别是在入侵者没有



经验的情况下更是如此。系统管理员通过运行强有力的登录工具，可使入侵者很难逃避检查，除非入侵者有较多的专业知识。

4. 允许未经授权的远程主机访问网络的漏洞

这种允许远程用户未经授权访问的漏洞，属于 A 类，是威胁性最大的一种漏洞。这类漏洞从外部对系统造成严重的威胁。在许多情况下，如果系统管理员只运行了很少的日志，这些攻击可能不会被记录下来，从而使捕捉更为困难。但采用搜索器便可以检查这些漏洞。因此，尽管安全程序员把这些漏洞包含进他们的搜索器程序中作为检查的选择，这些规则也总是在漏洞出现一段时间后才被制定出来。

大多数的 A 类漏洞是由于较差的系统管理或设置失误造成的。典型的设置错误是在驱动器上任意存放的脚本例程。这些脚本有时会为网络入侵者提供一些访问权限，有时甚至提供超级用户访问权限，如 Test.cgi 文件的缺陷是允许网络入侵者读取 CGI 目录下的文件。要补救该类漏洞，建议删除这些脚本。例如，Novell 平台上的一种 HTTP 服务器含有一个称为 Convert.bas 的例子脚本，这个用 BASIC 语言编写的脚本允许远程用户读取系统上的任何文件，删除该脚本即可避免远程用户读取系统上的任何文件。

入侵者利用脚本获取访问权。例如，Microsoft 的 IIS(Internet Information Server，因特网信息服务器)包含一个允许任何远程用户执行任意命令的漏洞。因为 IIS 中的 HTTP 将所有.bat 或.cmd 后缀的文件与 CMD 和 EXE 程序联系起来，入侵者如果能够执行 CMD 和 EXE 文件，那么就可以执行任何命令读取任意分区的任意文件。

3.1.3　漏洞对网络安全的影响

随着网络经济时代的到来，网络将会成为一个无处不在、无所不用的工具，经济、文化、军事和社会活动将会强烈地依赖于网络。因此，网络的安全性和可靠性已成为世界各国共同关注的焦点。而 Internet 的无主管性、跨国界性、不设防性、缺少法律约束性的特点，在为各国带来发展机遇的同时，也带来了巨大的风险。目前，Internet 和 Web 站点无数的风险事例已使一些用户坐立不安了，在他们看来，似乎到处都有漏洞，到处都是黑客的踪迹。事实正是如此，各种系统漏洞正严重地影响着 Internet 的安全。

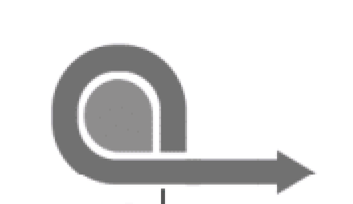
Netscape 通信和 Netscape 商业服务器也都有类似的漏洞。对于 Netscape 服务使用 BAT 或 CMD 文件作为 CGI 脚本则会发生上述类似的情况。

1. 漏洞影响 Internet 的可靠性和可用性

Internet 的网络脆弱性也是一种漏洞。Internet 是逐步发展和演变而来的，其可靠性和可用性存在很多弱点，特别是在网络规模迅速扩大、用户数目猛增、业务类型多样化的情况下，系统资源的不足已成为一个瓶颈，而系统和应用工具可靠性的弱点也逐渐暴露出来。随着经济和管理活动对网络依赖程度的加深，网络的故障和瘫痪将会给国家、组织和企业造成巨大的损失。

2. 漏洞导致了 Internet 上黑客入侵和计算机犯罪

黑客攻击早在主机——终端时代就已经出现，随着 Internet 的发展，现代黑客则从以系统为主的攻击转变到以网络为主的攻击，形形色色的黑客和攻击者利用网络上的任何漏洞



和缺陷进行攻击。例如，通过网络监听获取网上用户的账号和密码；监听密钥分配过程，攻击密钥管理服务器，得到密钥或认证码，从而取得合法资格；利用 Linux 操作系统中的 Finger 等命令收集信息，提高自己的攻击能力；利用 FTP，采用匿名用户访问进行攻击；利用 NFS 进行攻击；通过隐蔽通道进行非法活动；突破防火墙等。显然，黑客入侵和计算机犯罪给 Internet 的安全造成了严重的威胁。

3. 漏洞致使 Internet 遭受网络病毒和其他软件的攻击

自计算机病毒被发现以来，其种类以几何级数增长，而且病毒的机理和变种的不断演变为检测和消除带来了更大的难度，已成为计算机和网络发展的一大公害。计算机病毒破坏计算机的正常工作及信息的正常存储，严重时可以使计算机系统陷于瘫痪。

总之，漏洞对于 Internet 安全性的影响是非常严重的。不采取措施对漏洞进行补救，将严重地制约 Internet 的发展。

3.2 Windows Server 2003 的安全

众所周知，微软公司的 Windows Server 2003 操作系统因其操作方便、功能强大而成为新一代服务器操作系统的主流，越来越多的应用系统运行在 Windows Server 2003 操作系统上。在日常工作中，有的管理员在安装和配置操作系统时不注意做好安全防范工作，导致系统安装结束的同时，计算机病毒也入侵到操作系统里了。如何才能搭建一个安全的操作系统是安全管理人员所关心的一个问题，同时 Windows Server 2003 也自然就成为了黑客攻击的对象。

3.2.1 Windows Server 2003 安全模型

Windows Server 2003 操作系统安全模型的主要功能是用户身份验证和访问控制。Active Directory 目录服务确保管理员可轻松、有效地管理这些功能。

1. 身份验证

Windows Server 2003 家族中身份验证的重要功能就是它对单一登录的支持。单一登录允许用户使用一个密码一次登录到域，然后向域中的任何计算机验证身份。

1) 单一登录

单一登录在安全性方面提供了两个主要优点。

(1) 对用户而言，单个密码或智能卡的使用减少了混乱，提高了工作效率。

(2) 对管理员而言，由于管理员只需要为每个用户管理一个账户，所以域用户所要求的管理支持减少了。

2) 身份验证(包括单一登录)

身份验证分两部分执行：交互式登录；网络身份验证。成功的用户身份验证取决于这两个过程。

交互式登录过程向域账户或本地计算机确认用户的身份，这一过程根据用户账户的类型不同而不同。

(1)　使用域账户。用户可以通过存储在 Active Directory 目录服务中的单一登录凭据使用密码或智能卡登录到网络。如果使用域账户登录，被授权的用户可以访问该域以及任何信任域中的资源；如果使用密码登录到域账户，系统将使用 Kerberos V5 进行身份验证；如果使用智能卡，则需要将 Kerberos V5 身份验证和证书一起使用。

(2)　使用本地计算机账户。用户可以通过存储在安全账户管理器(SAM)(也就是本地安全账户数据库)中的凭据登录到本地计算机。任何工作站或成员服务器均可以存储本地用户账户，但这些账户只能用于访问该本地计算机。

网络身份验证向用户尝试访问的任何网络服务去确认用户的身份证明。为了提供这种类型的身份验证，安全系统支持多种不同的身份验证机制，包括 Kerberos V5、安全套接字层/传输层安全性(SSL/TLS)以及为了与 Windows NT 4.0 兼容而提供的 NTLM。

网络身份验证对于使用域账户的用户来说不可见。使用本地计算机账户的用户每次访问网络资源时，必须提供凭据，如用户名和密码。通过使用域账户，用户就具有了可用于单一登录的凭据。

2. 访问控制概述

访问控制是批准用户、组和计算机访问网络上对象的过程。构成访问控制的主要概念是权限、用户权力和对象审核。

1)　权限

权限定义了授予用户或组对某个对象或对象属性的访问类型。例如，Finance 组可以被授予对名为 Payroll.dat 文件的“读取”和“写入”权限。

权限应用到任何受保护的对象上，如文件、Active Directory 对象或注册表对象。权限可以授予任何用户、组或计算机，好的做法是将权限指派到组。

可以将对象的权限指派到：

- 域中的组、用户和特殊标识符。
- 该域或任何受信任域中的组和用户。
- 对象所在的计算机上的本地组和用户。
- 附加在对象上的权限取决于对象的类型。例如，附加给文件的权限与附加给注册表项的权限不同。但是，某些权限对于大多数类型的对象都是公用的。这些公用权限有：读取权限；修改权限；更改所有者；删除。

设置权限，就是为组和用户指定访问级别。例如，可以允许一个用户读取文件的内容，允许另一个用户修改该文件，同时防止所有其他用户访问该文件；可以在打印机上设置类似的权限，使某些用户可以配置打印机，而其他用户只能用其打印。

如果需要更改个别对象的权限，只要启动适当的工具和更改对象的属性即可。例如，要更改文件的权限，可以启动 Windows 资源管理器，右击文件名，然后在弹出的快捷菜单中选择【属性】命令。在弹出的对话框中切换到【安全】选项卡更改文件的权限。

- 对象的所有权：在创建对象时，即有一个所有者指派给该对象。所有者被默认为对象的创建者，不管为对象设置什么权限，对象的所有者总是可以更改对象的权限。
- 权限的继承：继承使得管理员易于指派和管理权限。该功能自动使容器中的对象



继承该容器的所有可继承权限。例如，文件夹中的文件一经创建就继承了文件夹的权限，当然只继承标记为要继承的权限。

2) 用户权力

用户权力授予计算机环境中的用户和组具有特定的特权和登录权力。

3) 对象审核

可以审核用户对对象的访问情况，即可以使用事件查看器在安全日志中查看这些与安全相关的事件。

3. 加密文件系统

加密文件系统(EFS)提供一种核心文件加密技术，该技术用于在 NTFS 文件系统卷上存储已加密的文件。加密文件或文件夹后，就可以像使用其他文件和文件夹一样使用它们了。

加密文件系统对加密该文件的用户是透明的。这表明不必在使用前手动解密已加密的文件，就可以正常打开和更改文件。

使用 EFS 类似于使用文件和文件夹上的权限。两种方法都可用于限制数据的访问。然而，未经许可对加密文件和文件夹进行物理访问的入侵者将无法阅读这些文件和文件夹中的内容。如果入侵者试图打开或复制已加密的文件或文件夹，将收到拒绝访问的消息。文件和文件夹上的权限不能防止未授权的物理攻击。

正如设置其他任何属性(如只读、压缩或隐藏)一样，通过为文件夹和文件设置加密属性，可以对文件夹或文件进行加密和解密。如果加密一个文件夹，则存在于加密文件夹中创建的所有文件和子文件夹都自动加密，因而推荐在文件夹级别上加密。

在使用加密文件和文件夹时，应该注意以下问题。

(1) 只有 NTFS 卷上的文件或文件夹才能被加密。由于 WebDAV 使用 NTFS，当通过 WebDAV(Web 分布式创作和版本控制)加密文件时需用 NTFS。

(2) 不能加密压缩的文件或文件夹。如果用户加密某个压缩文件或文件夹，则该文件或文件夹将会被解压。

(3) 如果将加密的文件复制或移动到非 NTFS 格式的卷上，该文件将会被解密。

(4) 如果将非加密文件移动到加密文件夹中，则这些文件将在新文件夹中自动加密。然而，反向操作则不能自动解密文件，文件必须被明确解密。

(5) 无法加密标记为“系统”属性的文件，并且对位于 System Root 目录结构中的文件也无法加密。

(6) 加密文件夹或文件不能防止删除或列出文件或目录。具有合适权限的人员可以删除或列出已加密文件夹或文件。因此，建议结合 NTFS 权限使用 EFS。

(7) 在允许进行远程加密的远程计算机上可以加密或解密文件及文件夹。然而，如果通过网络打开已加密文件，通过此过程在网络上传输的数据并未加密，必须使用诸如 SSL/TLS(安全套接字层/传输层安全性)或 Internet 协议安全性(IPSec)等其他协议通过有线加密数据。但 WebDAV 可在本地加密文件并采用加密格式发送。

4. 公钥基础结构

计算机网络已不再是用户只要连在网络上就能证实其身份的封闭系统。在这个信息互联的时代，一个单位的网络可能包括内部网、Internet 站点和外部网，所有这些都有可能被

一些未经授权的个人访问，他们会蓄意盗阅或更改该单位的数据。

系统管理员如何才能确认访问信息人的标识及给定该标识呢？如何控制哪个人有权访问哪些信息呢？此外，系统管理员如何才能轻松并安全地跨全单位地分发和管理标识凭据呢？这些问题都可以通过规划良好的公钥基础结构来解决。

有许多潜在的机会在未经授权时即可访问网络上的信息。个人可以尝试监视或更改类似于电子邮件、电子商务和文件传输这样的信息流。一个单位可能与合作伙伴在限定的范围和时间内进行项目合作，有些雇员虽然对此一无所知，但却必须给他们一定的权限访问你的部分信息资源。如果用户为了访问不同安全系统需要记住许多密码，他们可能选择一些防护性较差或很普通的密码，以便于记忆。这就不仅给黑客提供了一个容易破解的密码，而且还使他们能够访问众多安全系统和存储的数据。

公钥基础结构(PKI)是通过使用公钥加密对参与电子交易的每一方的有效性进行验证和身份验证的数字证书、证书颁发机构(CA)和其他注册机构(RA)。尽管 PKI 的各种标准正被作为电子商务的必需元素来广泛实现，但它们仍在发展。

5. Internet 协议安全性定义

“Internet 协议安全性(IPSec)”是一种开放标准的框架结构，通过使用加密的安全服务以确保在 Internet 协议(IP)网络上进行保密而安全的通信。Windows Server 2003 家族、Windows XP 实施的 IPSec 基于的是“Internet 工程任务组”(IETF)的 IPSec 工作组开发的标准。

IPSec 是安全联网的长期方向。它通过端对端的安全性来提供主动的保护以防止来自专用网络与 Internet 的攻击。在通信中，只有发送方和接收方才是唯一必须了解 IPSec 保护的计算机。在 Windows XP 和 Windows Server 2003 家族中，IPSec 提供的功能可用于保护工作组、局域网计算机、域客户端和服务器、分支机构(可能在物理上为远程机构)、Extranet 及漫游客户端之间的通信。

3.2.2　Windows Server 2003 安全隐患

上面介绍了 Windows Server 2003 中采取的一些安全措施，但在实际应用中，仍然出现了许多新的安全问题。

1. 安装隐患

在一台服务器上安装 Windows Server 2003 操作系统时，主要存在以下隐患。

(1) 将服务器接入网络内安装。Windows Server 2003 操作系统在安装时存在一个安全漏洞，即当输入 Administrator 密码后，系统就自动建立了 ADMIN$的共享，但是并没有用刚刚输入的密码来保护它，这种情况一直持续到再次启动后。在此期间，任何人都可以通过 ADMIN$进入这台机器。同时，只要安装一结束，各种服务就会自动运行，而这时的服务器自身充满了漏洞，计算机病毒非常容易侵入。因此，将服务器接入网络内安装是极为错误的做法。

(2) 操作系统与应用系统共用一个磁盘分区。在安装操作系统时，将操作系统与应用系统安装在同一个磁盘分区，会导致一旦操作系统文件泄露时，攻击者可以通过操作系统



漏洞获取应用系统的访问权限，从而影响应用系统的安全运行。

(3) 采用 FAT32 文件格式安装。FAT32 文件格式不能限制用户对文件的访问，这样可能导致系统的不安全。

(4) 采用默认安装。默认安装操作系统时，会自动安装一些有安全隐患的组件，如 IIS、DHCP、DNS 等，从而导致系统在安装后存在安全漏洞。

(5) 系统补丁安装不及时、不全面。在系统安装完成后，不及时安装系统补丁程序，从而导致病毒侵入。

2. 运行隐患

在系统运行过程中，主要存在以下隐患。

(1) 默认共享。在系统运行后，会自动创建一些隐藏的共享：一是 CDE$每个分区的根共享目录；二是 ADMIN$远程管理用的共享目录；三是 IPC$空连接；四是 NetLogon 共享；五是其他系统默认共享，如 FAX$、PRINT$共享等。这些默认共享给系统的安全运行带来了很大的隐患。

(2) 默认服务。系统在运行后，自动启动了许多有安全隐患的服务，如 Telnet Services、DHCP Client、DNS Client、Print Spooler、Remote Registry services(选程修改注册表服务)、SNMP Services、Terminal Services 等。如果这些服务在实际工作中不需要，可以禁用。

(3) 安全策略。系统运行后，默认情况下，系统的安全策略是不起作用的，因此降低了系统的运行安全性。

(4) 管理员账号。系统在运行后，Administrator 用户的账号是不能被停用的，这意味着攻击者可以一遍又一遍地尝试猜测这个账号的口令。此外，设置简单的用户账号口令也给系统的安全运行带来了隐患。

(5) 页面文件。页面文件用来存储没有装入内存的程序和数据文件部分的隐藏文件。页面文件中可能含有一些敏感的资料，因而有可能造成系统信息的泄露。

(6) 共享文件。默认状态下，每个人对新创建的文件共享都拥有完全的控制权限，这是非常危险的，应严格限制用户对共享文件的访问。

(7) Dump 文件。Dump 文件在系统崩溃和蓝屏的时候是一份很有用的查找问题的资料。然而，它也能够给攻击者提供一些敏感信息，比如一些应用程序的口令等，从而造成信息泄露。

(8) Web 服务。系统本身自带的 IIS 服务、FTP 服务存在安全隐患，容易导致系统被攻击。

3.2.3 Windows Server 2003 安全防范措施

虽然 Windows Server 2003 稳定的性能受到越来越多用户的青睐，但面对层出不穷的新病毒，加强安全性依旧是当务之急。通常，只需做一些改动就能使系统的安全性提升一个台阶。

1. 安装对策

在安装系统时，需要采取以下对策。

(1) 在完全安装、配置好操作系统，并安装系统补丁之前，不要把机器接入网络。

(2) 在安装操作系统时，建议至少划分 3 个磁盘分区。第一个分区用来安装操作系统，第二个分区存放 IIS、FTP 和各种应用程序，第三个分区存放重要的数据和日志文件。

(3) 采用 NTFS 文件格式安装操作系统，可以保证文件的安全，并能自由地控制用户对文件的访问权限。

(4) 在安装系统组件时，不要采用默认安装，要删除系统默认选中的 IIS、DHCP、DNS 等服务。

(5) 在安装完操作系统后，应先安装应用程序，再安装系统补丁。安装的系统补丁一定要全面。

2. 运行对策

在系统运行时，应采取以下对策。

1) 关闭系统默认共享

方法一：采用批处理文件在系统启动后自动删除共享。首先在 COMMAND 提示符下输入 Net Share 命令，查看系统自动运行的所有共享目录。然后建立一个批处理文件 sharedel.bat，并将该批处理文件放入计划任务中，设置为每次开机时运行。文件内容如下。

```
NETSHAREC$/DELETE
NETSHARED$/DELETE
NETSHAREE$/DELETE
......
NETSHAREIPC$/DELETE
NETSHAREADMIN$/DELETE
```

方法二：修改系统注册表，禁止默认的共享功能。在 Local_Machine\System\CurrentControlSet\Services\Lanmanserver\parameter 下新建一个双字节项 auto share server，设置其值为 0 即可。

2) 删除不需要的网络协议

删除网络协议中的 N Link Net BIOS 协议、NWLink IPX/SPX/NetBIOS 协议，NeBEUIPROtocol 协议和服务等，只保留 TCP/IP 网络通信协议。

3) 关闭不必要的有安全隐患的服务

可以根据实际情况，关闭表 3.1 中列出的服务。这些服务是系统自动运行的有安全隐患的服务。

表 3.1　需要关闭的服务表

服务名称	更改操作
DHCP Client	停止并禁用
DNS Client	停止并禁用
Print spooler	停止并禁用



续表

服务名称	更改操作
Remote Registry services	停止并禁用
SNMP services	停止并禁用
Telnet services	禁用
Terminal services	禁用

4) 启用安全策略

安全策略包括以下两个方面。

(1) 账号锁定策略。设置账号锁定阈值，比如 5 次无效登录后，即锁定账号。

(2) 密码策略。

操作系统的密码(口令)十分重要，它是抵抗攻击的第一道防线，因此必须把密码安全作为安全策略的第一步。安全的密码至少要具备以下 4 个条件中的 3 个：大写字母、小写字母、数字、非字母数字的字符(如标点符号等)。

安全的密码还要符合下列规则：不使用普通的名字或昵称；不使用普通的个人信息，如生日日期，密码里不含有重复的字母或数字，至少使用 8 个字符。另外，还应该定期修改密码。

以下举例说明强壮密码的重要性：假设密码设置为 6 位(包括任意 5 个字母和一位数字或符号)，则其可能性将近有 163 亿种。不过这只是理论估算，实际上密码比这有规律得多。例如，英文常用词条约 5000 条，从 5000 个词中任取一个字母与一个字符合成口令，仅有 688 万种可能性，在一台 600MHz 的计算机上每秒可运算 10 万次，则破解时间仅需 1min，即使采用穷举方法，也只需 9h，因此 6 位密码十分不可靠。而对于 8 位密码(包括 7 个字母和 1 位数字或符号)来说，若要完全破解，则需要将近 3 年的时间。因此，密码不要用全部数字、自己的中英文名、字典上的词，一定要使用数字和字母交替夹杂，并最好加入@#$%!&*?之类的字符。

【例 3.1】 使用安全强壮的密码。

Windows Server 2003 系统在默认配置下允许任何字符或字符串作为密码，包括空格，这是相当不安全的，可以通过修改注册表使得设定的密码中必须同时包含字母和数字，从而增强系统的安全性。

(1) 选择【控制面板】|【管理工具】|【本地安全策略】命令，打开【本地安全设置】窗口，如图 3.1 所示。

(2) 选择【账户策略】中的【密码策略】选项，双击想要更改的项目，比如【密码长度最小值】，打开图 3.2 所示的【密码长度最小值 属性】对话框。

(3) 设置好对应的内容，单击【确定】按钮。

还可以按照上面的步骤作表 3.2 所示的设置。

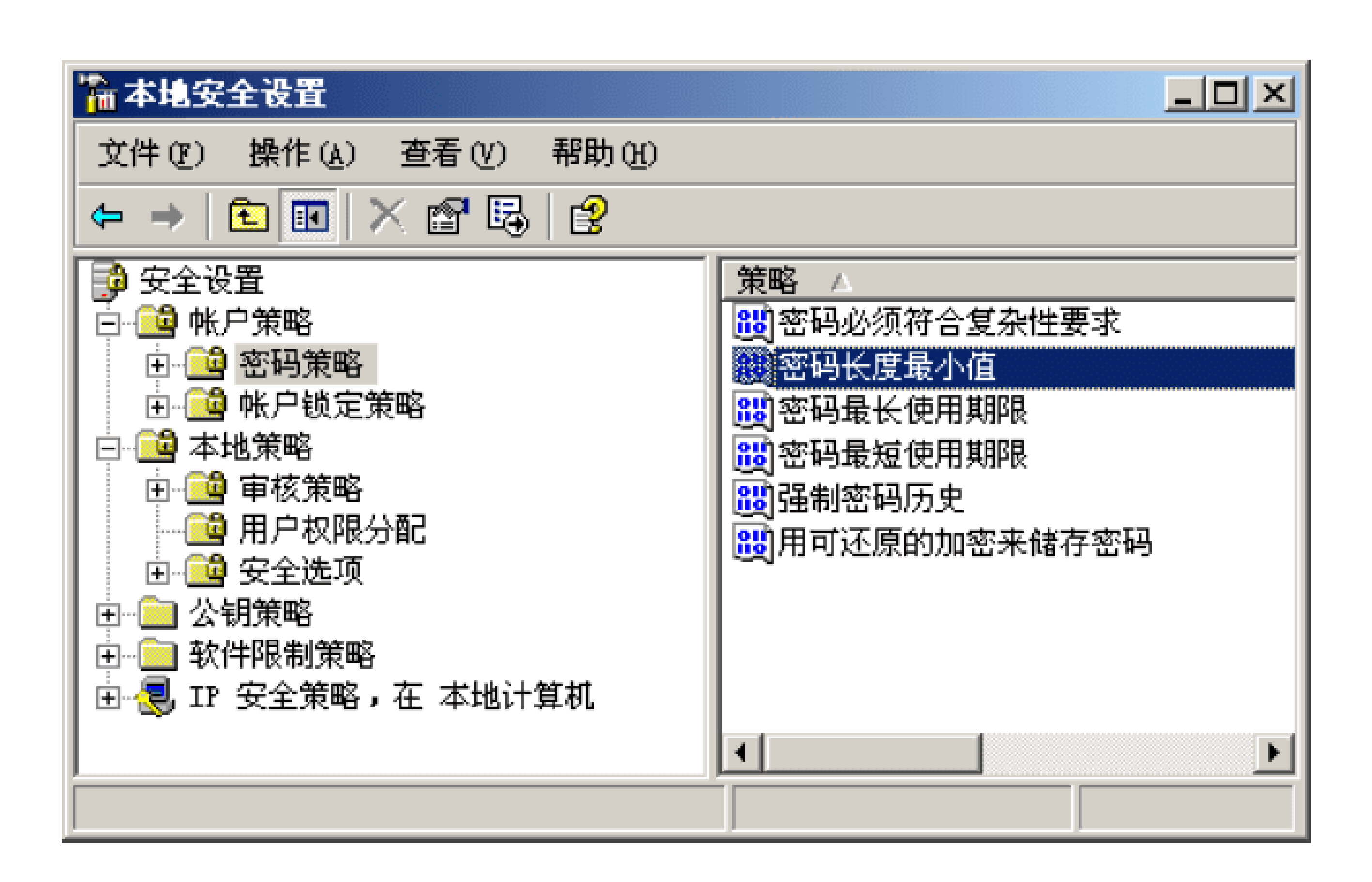


图 3.1　【本地安全设置】窗口

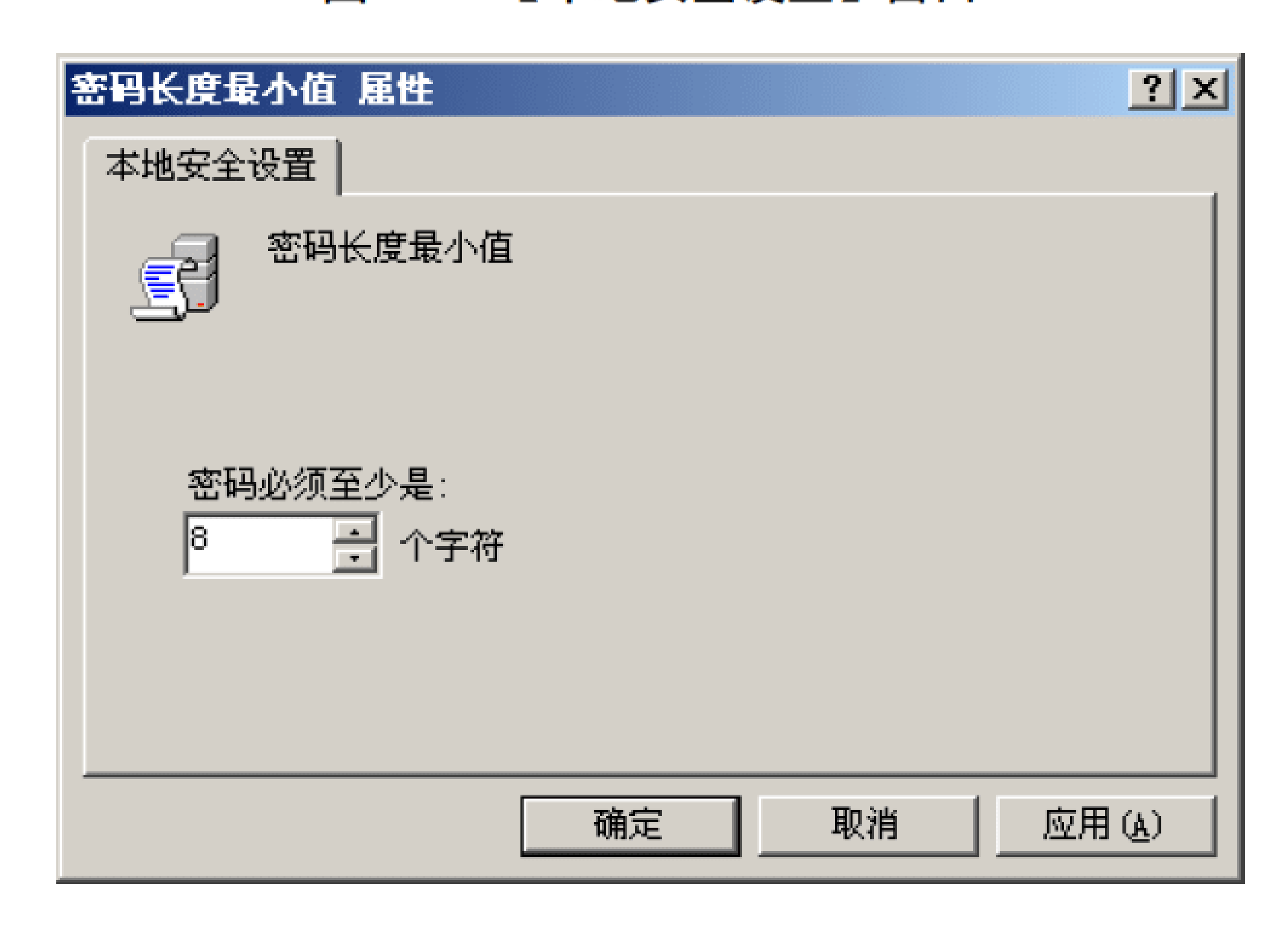


图 3.2　【密码长度最小值 属性】对话框

表 3.2　密码策略设置

策　略	安全设置
密码复杂性要求	启用
密码长度最小值	8 位
强制密码历史	5 次
强制密码历史	42 天

注：后两项会因操作系统的不同，设置名称等会不尽相同，但意义都一样。

3. 重新启动计算机使新的设置生效

1)　审核策略

默认安装时审核策略是关闭的。激活此功能有利于管理员很好地掌握机器的状态，有利于系统的入侵检测。可以从日志中了解到计算机是否在被攻击、是否有非法的文件访问等。开启安全审核是系统最基本的入侵检测方法。当攻击者尝试对系统进行某些方式(如尝试用户口令、改变账号策略、未经许可的文件访问等)入侵时，都会被安全审核记录下来。

下面的这些审核是必须开启的，其他的可以根据需要增加如图 3.3 所示：审核系统登



录事件、审核账户管理、审核登录事件、审核对象访问、审核策略更改、审核特权使用、审核系统事件。

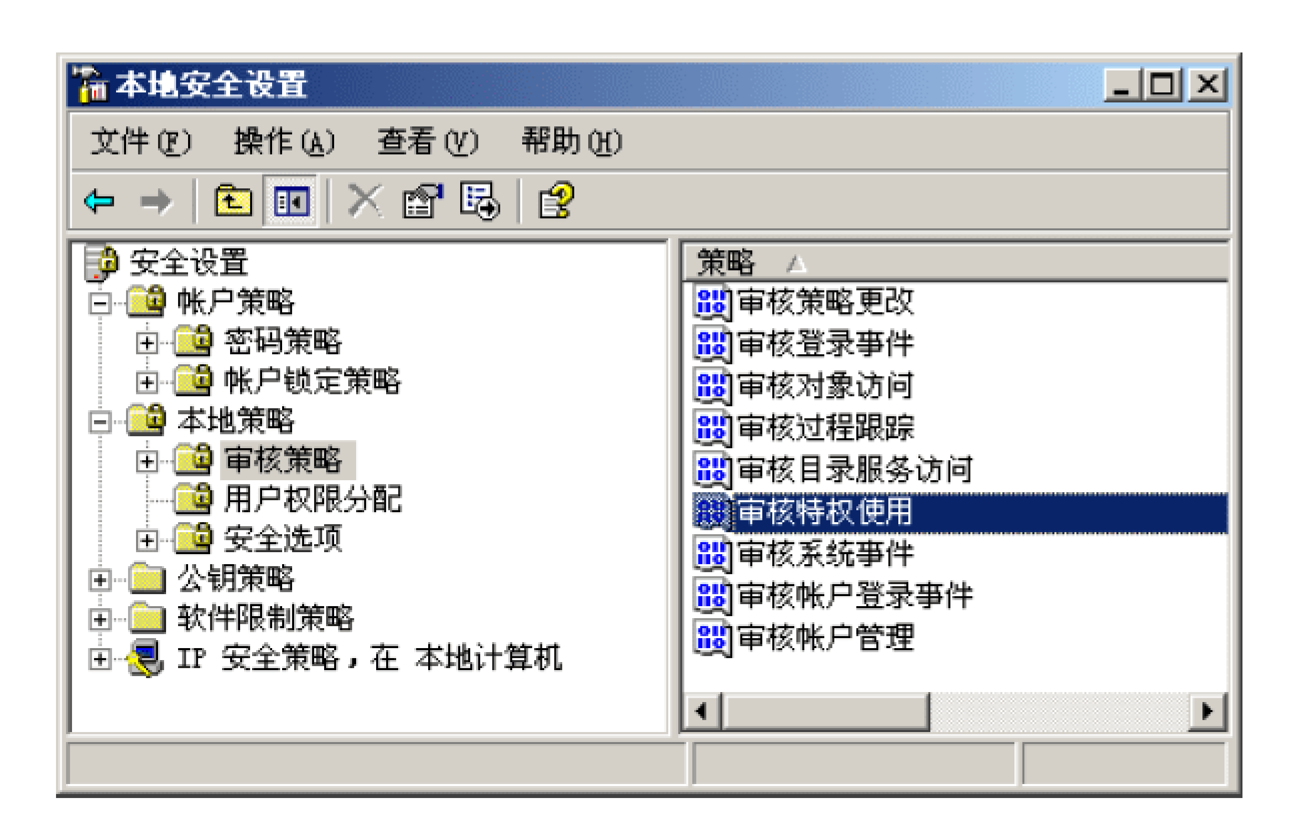


图 3.3 审核策略设置

2) 用户权限分配

3) 安全选项

在【安全选项】中，右击【网络访问：不允许枚举 SAM 账户和共享的匿名枚举】选项，在弹出的快捷菜单中选择【属性】命令，打开【网络访问：不允许 SAM 账户和共享的匿名枚举 属性】对话框，将其属性设置为【已禁用】，如图 3.4 所示。

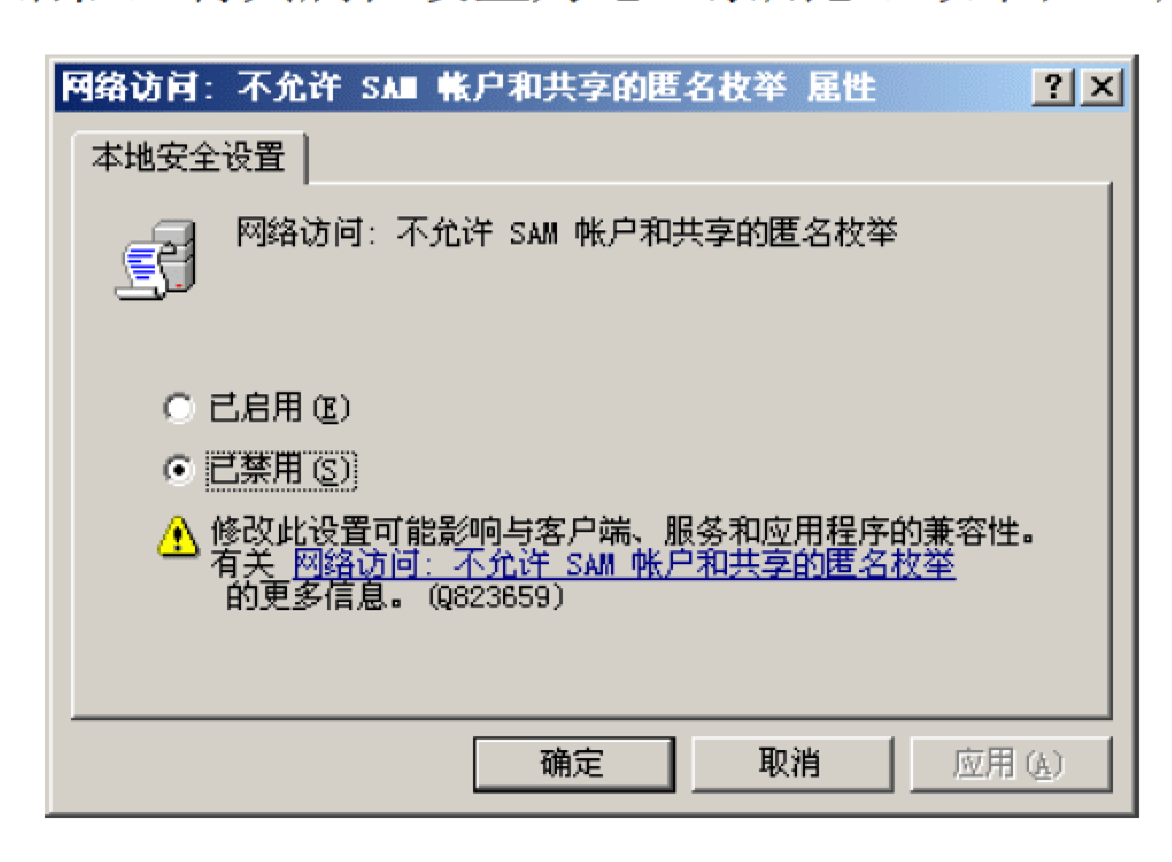


图 3.4 【网络访问：不允许 SAM 账户和共享的匿名枚举 属性】对话框

也可以通过修改注册表中的值来禁止建立空连接，选择【开始】|【运行】命令，打开【运行】对话框，输入 regedit.exe，打开【注册表编辑器】窗口，如图 3.5 所示，选择 Hkey_Local_Machine\ System\ CurrentControlSet\Control\Lsa 中的 restrictanonymous，右击打开快捷菜单，选择【修改】命令，打开【编辑 DWORD 值】对话框，将数值数据值改为 1，如图 3.6 所示。这可以有效地防止利用 IPC$空连接枚举 SAM 账号和共享资源，造成系统信息泄露。

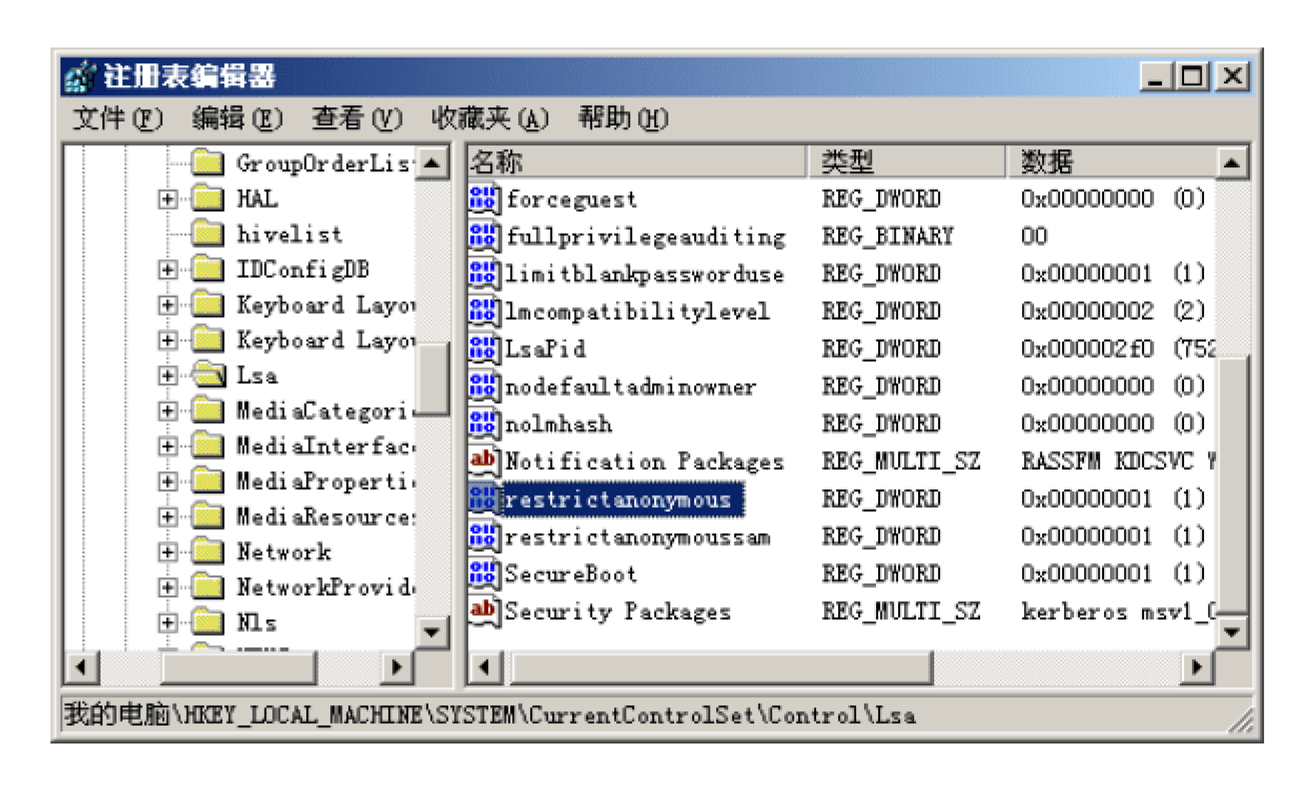


图 3.5　修改注册表中 restrictanonymous 的值



图 3.6　【编辑 DWORD 值】对话框

4. 加强对 Administrator 账户和 Guest 账户的管理监控

将 Administrator 账户重新命名，新建一个陷阱账号，名为 Administrator，口令为 10 位以上的复杂口令，其权限设置为最低，即将其设为不隶属于任何一个组，并通过安全审核，借此发现攻击者的入侵企图。设置两个管理员用账号：一个具有一般权限，用来处理一些日常事务；另一个具有管理员权限，只在需要的时候使用。修改 Guest 用户口令为复杂口令，或者禁用 Guest 用户账号。

5. 清除页面文件

选择【开始】|【运行】命令，打开【运行】对话框，输入 regedit.exe，打开【注册表编辑器】窗口，修改 HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\ MemoryManagement 中 Clear Page File At Shutdown 的值为 1，可以禁止系统产生页面文件，防止信息泄露，如图 3.7 所示。

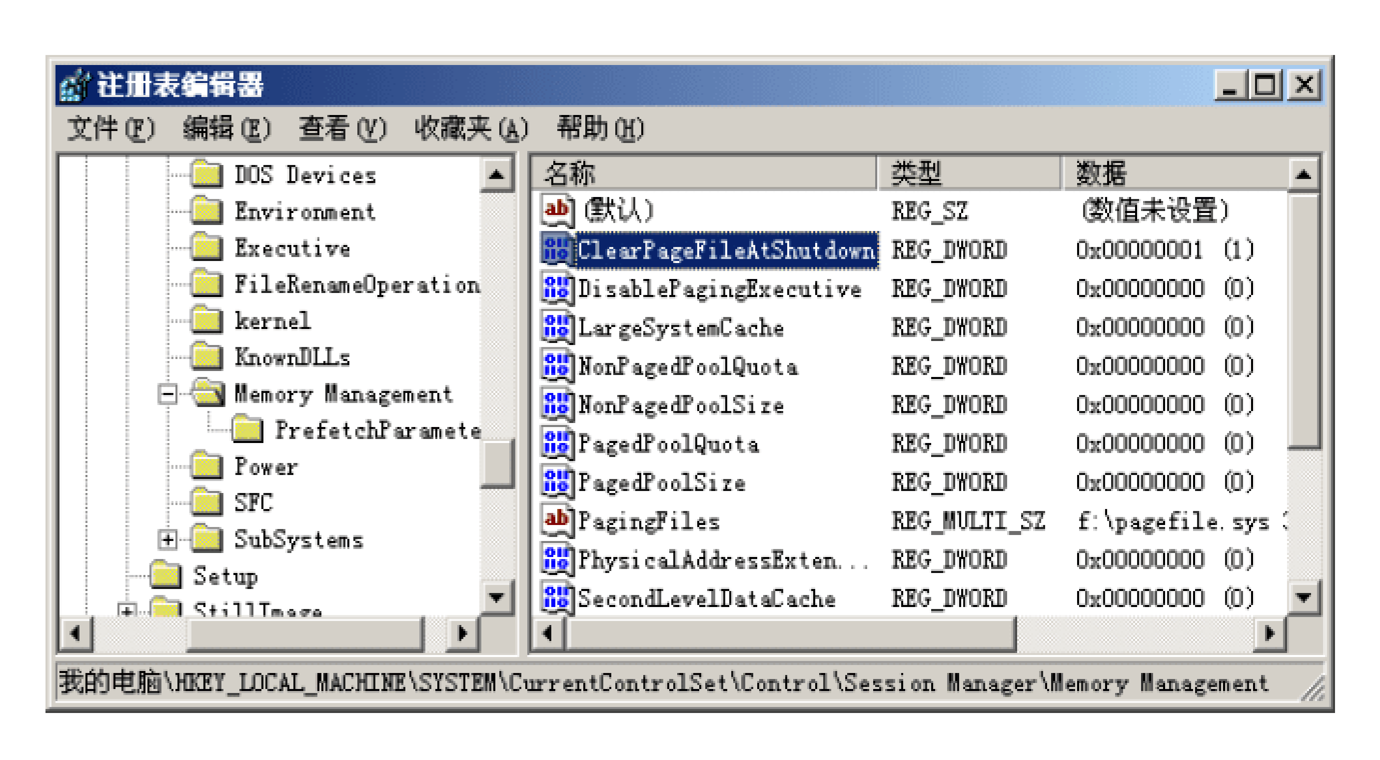


图 3.7　清除页面文件



6. 清除 Dump 文件

选择【控制面板】|【系统】|【高级】|【启动和故障恢复】命令，打开【启动和故障恢复】对话框，在【写入调试信息】选项组中的下拉列表框中选择【无】选项，可以清除 Dump 文件，防止信息泄露，如图 3.8 所示。

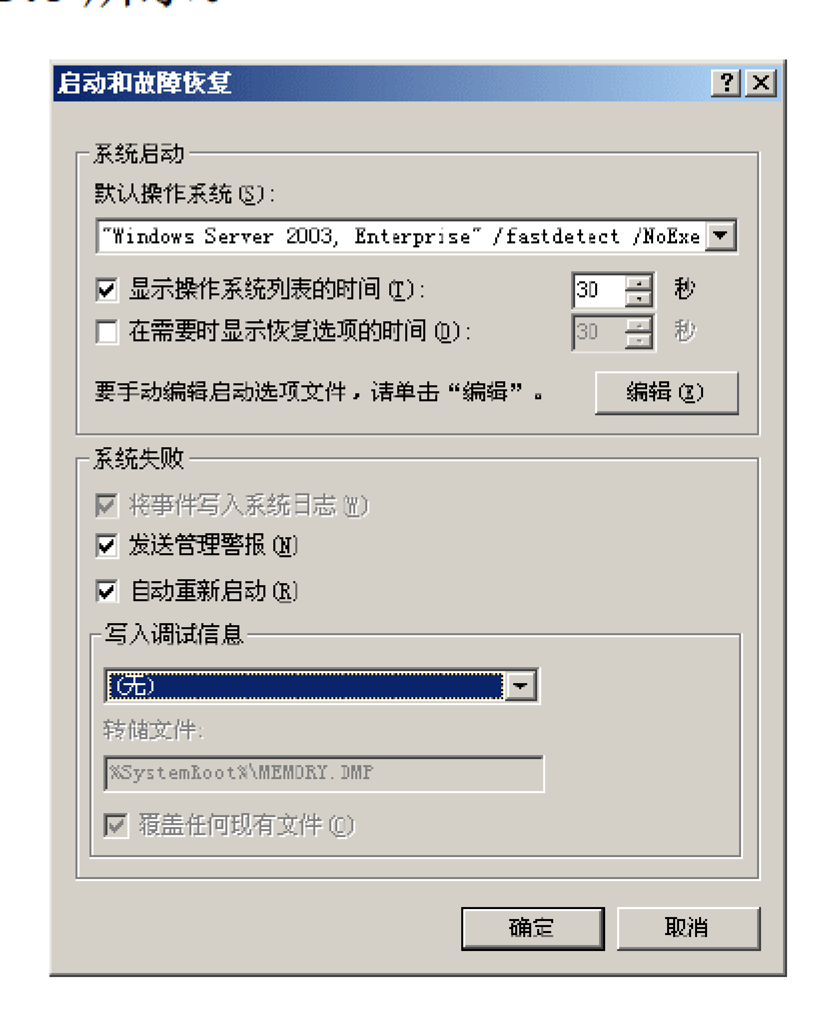


图 3.8　清除 Dump 文件

7. 防范 NetBIOS 漏洞攻击

在局域网内部使用 NetBIOS 协议可以非常方便地实现消息通信，但是如果在因特网上，NetBIOS 就相当于一个后门程序，很多攻击者都是通过 NetBIOS 漏洞发起攻击的。

NetBIOS(Network Basic Input Output System，网络基本输入输出系统)是一种应用程序接口(API)，系统可以利用 WINS(管理计算机 NetBIOS 名和 IP 映射关系)服务、广播及 Lmhost 文件等多种模式将 NetBIOS 名解析为相应的 IP 地址，从而实现信息通信。

【例 3.2】 对于 Windows Server 2003 系统而言，可以通过以下方式来设置。

(1) 选择【开始】|【设置】|【控制面板】|【网络和拨号连接】|【本地连接】命令，双击【Internet 协议(TCP/IP)】，打开如图 3.9 所示的【Internet 协议(TCP/IP)属性】对话框。

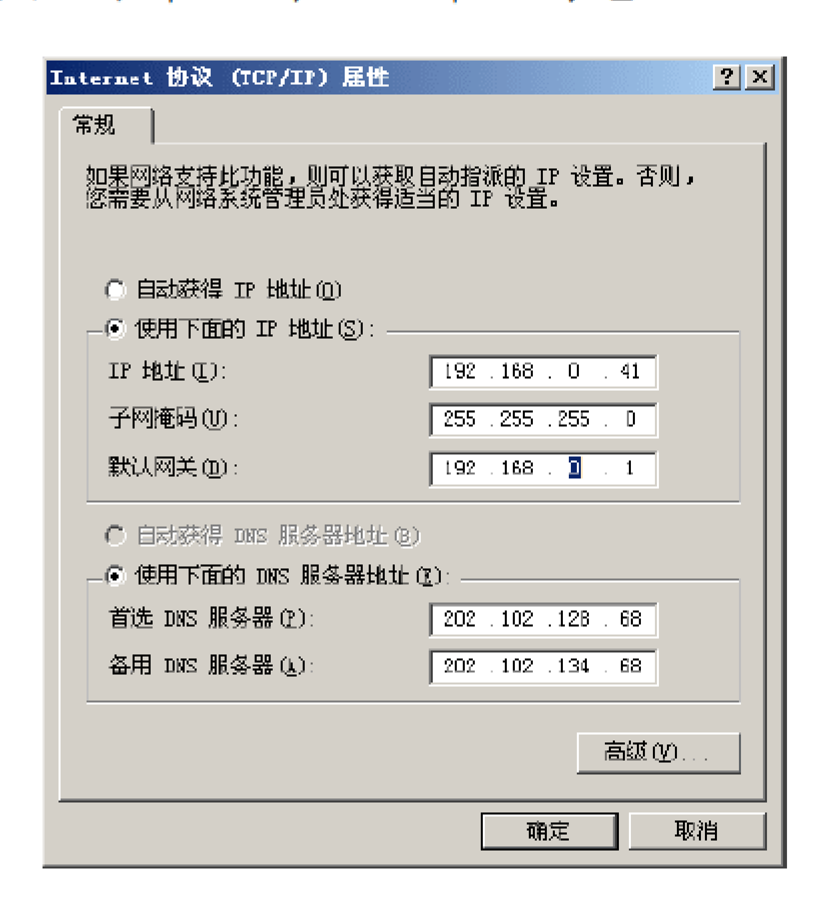


图 3.9　【Internet 协议(TCP/IP)属性】对话框

(2) 单击【高级】按钮，打开如图 3.10 所示的【高级 TCP/IP 设置】对话框，切换到【选项】选项卡。

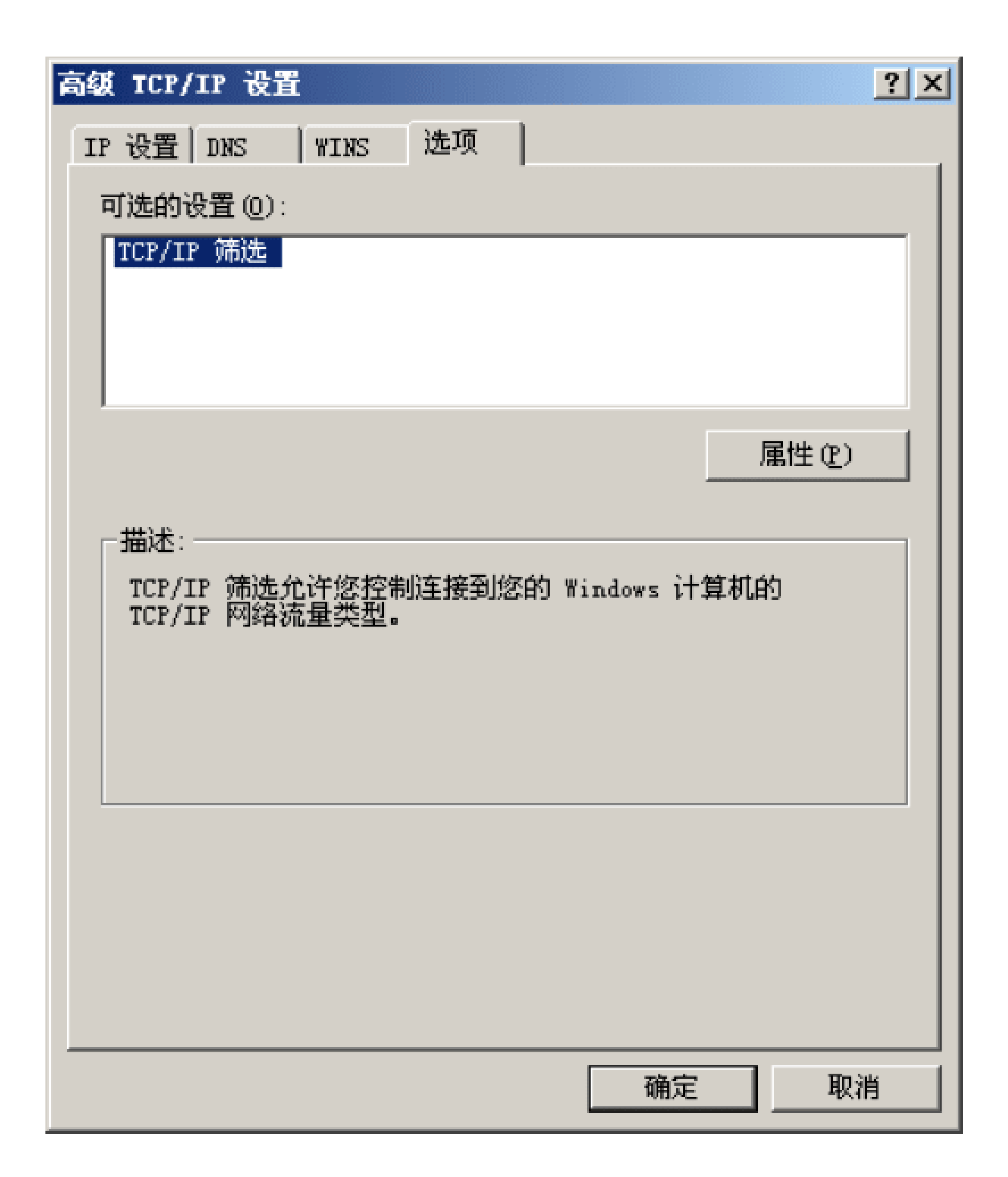


图 3.10 【高级 TCP/IP 设置】对话框

(3) 单击【属性】按钮，打开【TCP/IP 筛选】对话框，从中选中【启用 TCP/IP 筛选(所有适配器)】复选框，如图 3.11 所示。

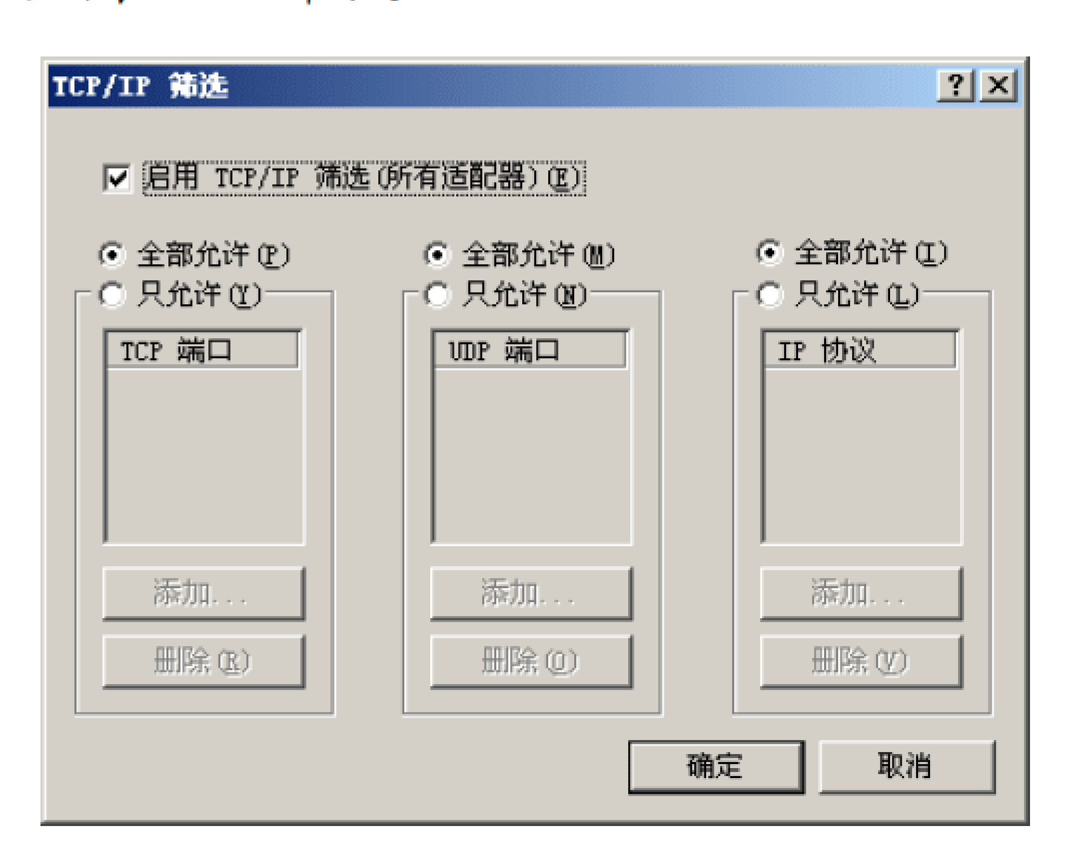


图 3.11 【TCP/IP 筛选】对话框

(4) 在【TCP 端口】中添加除了 139 之外要用到的服务端口即可。

8. Web 服务安全设置

对于 Web 服务和 FTP 服务的安全设置，建议采取以下措施。

(1) 在安装时不要选择 IIS 服务，安装完毕后手动添加该服务，将其安装目录设置为如 D:\INTE 等任意字符，以加大安全性。

(2) 删除 Internet 服务管理器，删除样本页面和脚本，卸载 Internet 打印服务，删除除 ASP 以外的应用程序映射。



(3) 针对不同类型文件建立不同文件夹并设置不同权限。

(4) 对脚本程序设置为纯脚本执行许可权限，二进制执行文件设置为脚本和可执行程序权限，静态文件设置为读权限。

(5) 对安全扫描出的 CGI 漏洞文件要及时删除。

9. 加固 IIS 服务器的安全

针对 Windows 系统的攻击几乎都偏重在 IIS 上，如 2001 年、2002 年的 Nimda、CodeRed 病毒等都是利用 IIS 漏洞入侵并且开始传播的。由于 Windows Server 2003 系统上使用 IIS 作为 WWW 服务程序居多，再加上 IIS 的脆弱性以及与操作系统的相关性，所以通过 IIS 的漏洞入侵来获得整个操作系统的管理员权限，对于一台未经安全配置的计算机来说是轻而易举的，因此，配置和管理好 IIS 在整个系统配置里就显得举足轻重。

IIS 的配置可以分为以下几个方面 (以下操作均是使用 Internet 信息服务管理器操作，可以在控制面板的管理工具里找到该快捷方式，如图 3.12 所示)。

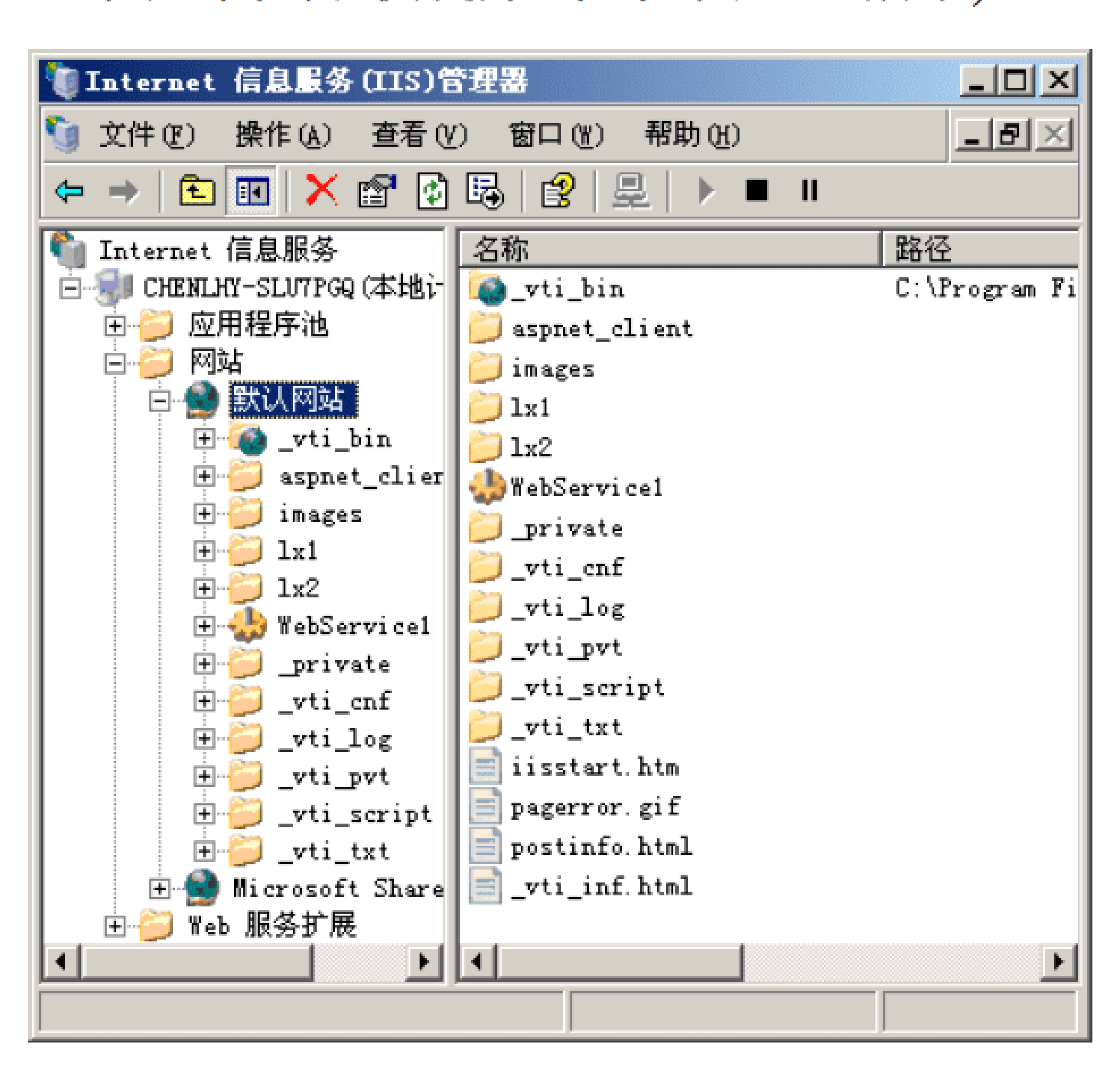


图 3.12 【Internet 信息服务(IIS)管理器】窗口

1) 删除目录映射

默认的 IIS 安装目录是 C:\inetpub，建议更改到其他分区的目录里面，比如 D:\inetpub 目录。

默认时 IIS 里有 Scripts、IISAdmin、IISSamples、MSADC、IISHelp、Printers 这些目录映射，建议完全删除 IIS 的默认映射目录，包括在服务器上真实的路径(%systemroot%是一个环境变量，在具体每台服务器上可能不一样，默认值由安装时选择目录决定)。

Scripts 对应 C:\inetpub\scripts 目录如下。

IISAdmin 对应%systemroot%\System32\inetsrv\iisadmin 目录。

IISSamples 对应 C:\inetpub\iissamples 目录。

MSADC 对应 C:\program files\common files\system\msadc 目录。

IISHelp 对应%systemroot%\help\iishelp 目录。

Printers 对应%systemroot%\Web\printers 目录。

IIS 管理员页面目录如下。

IISADMPWD 对应%systemroot%\system32\inetsrv\iisadmpwd 目录。

IISADMIN 对应%systemroot%\system32\inetsrv\iisadmin 目录。

2)　删除可执行文件扩展名(应用程序)映射

(1)　在【Internet 信息(IIS)服务管理器】窗口中，选择【默认网站】|【属性】选项，打开【默认网站 属性】对话框，如图 3.13 所示。



图 3.13　【默认网站 属性】对话框

(2)　在该对话框中单击【配置】按钮，默认有以下程序映射，如图 3.14 所示。

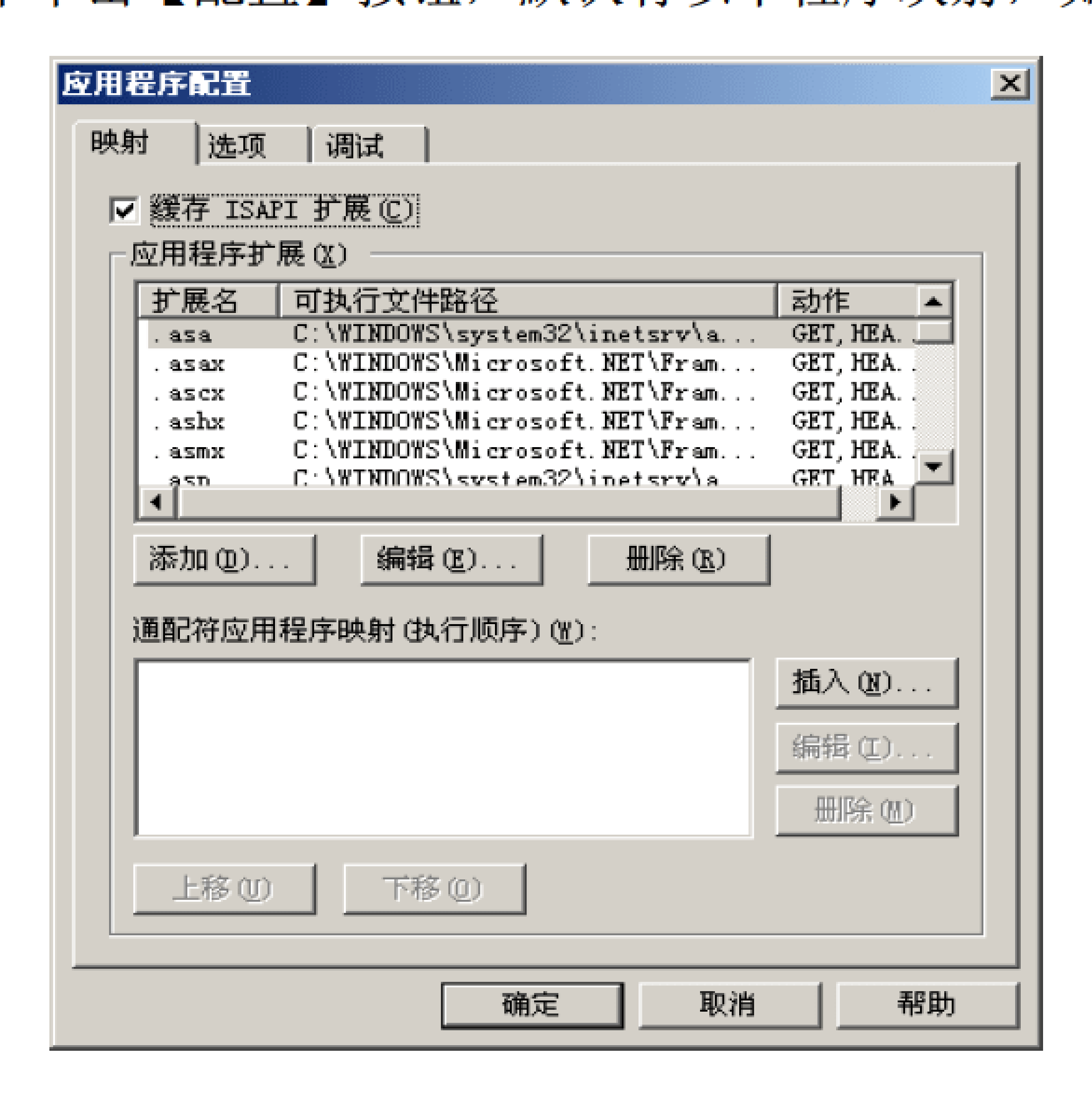


图 3.14　【映射】选项卡

如果不使用 SSI(side server include，服务器端嵌入脚本)，建议删除.shtm、.stm 和.shtml 这些映射文件，建议只保留.asp 和.asa 的映射。



3) Frontpage 扩展服务

(1) 选择【开始】|【设置】|【控制面板】命令，打开【控制面板】窗口，双击【添加或删除程序】图标，打开【添加或删除程序】对话框，选择【添加/删除 Windows 组件】选项，打开【windows 组件向导】对话框，如图 3.15 所示。

(2) 选中【应用程序服务器】复选框，单击【详细信息】按钮，打开【应用程序服务器】对话框，如图 3.16 所示。



图 3.15 【Windows 组件向导】对话框

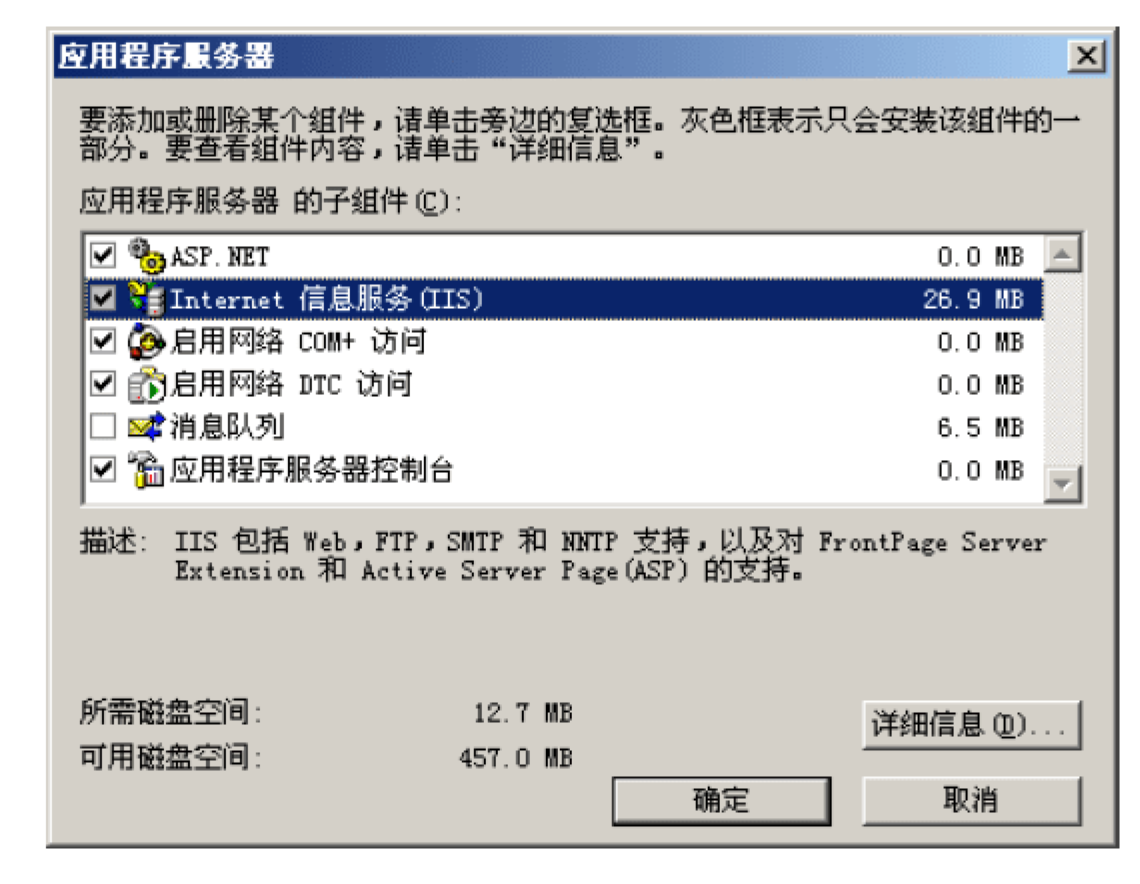


图 3.16 【应用程序服务器】对话框

(3) 选择【Internet 信息服务(IIS)】复选框，单击【详细信息】按钮，打开【Internet 信息服务(IIS)】对话框，确认 FrontPage 2002 Server Extensions 复选框未被选中，如图 3.17 所示，单击【确定】按钮。

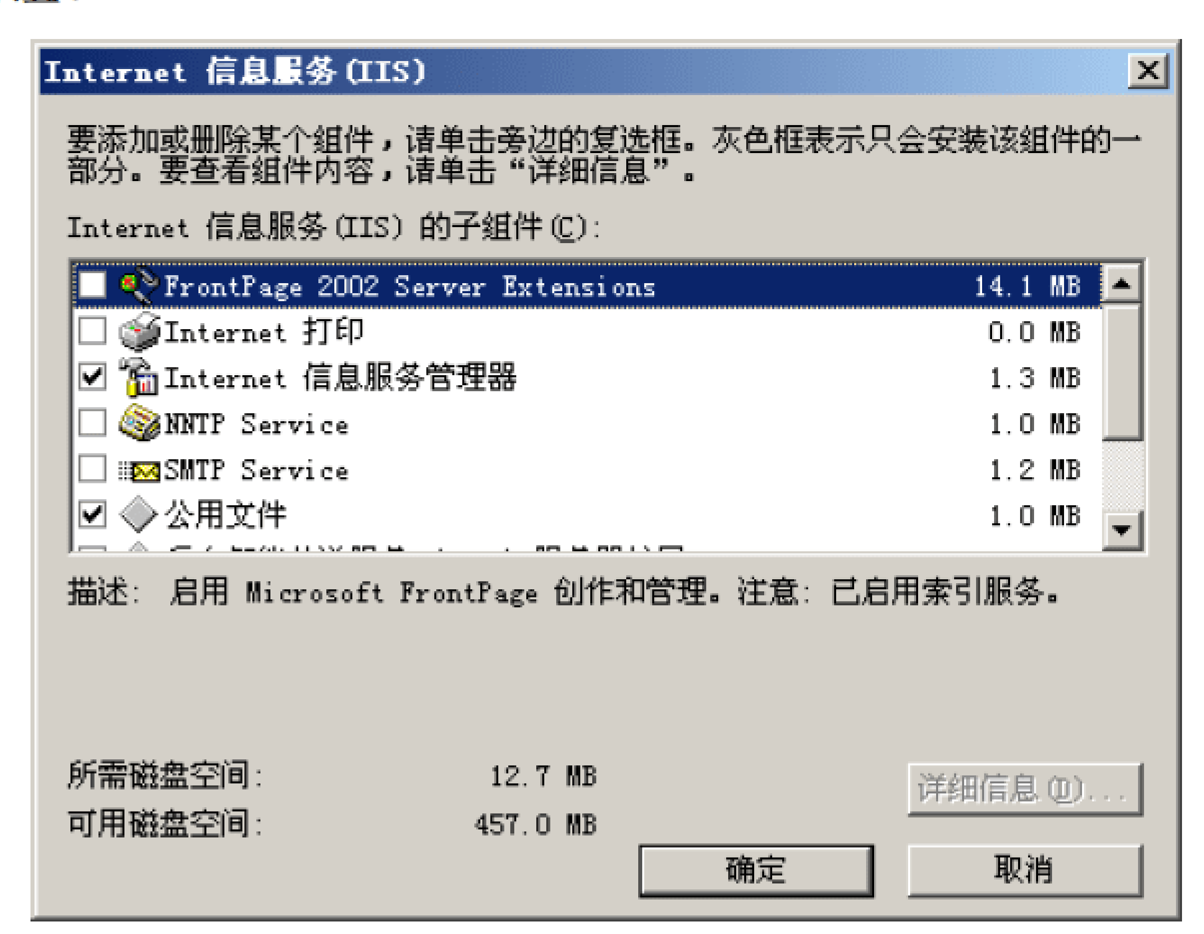


图 3.17 【Internet 信息服务(IIS)】对话框

4) FTP 文件传输服务

尽量不要使用系统自带的 FTP 服务，因为该服务与系统账户集成认证，一旦密码泄露后果十分严重。建议利用第三方软件 Serv-U 提供的 FTP 服务，该软件采用单向 Hash 函数(MD5)加密用户口令，加密后的口令保存在 ServUDaemon.ini 或是注册表中；用户权限管理采用多权限和模拟域方式，并且虚拟路径和物理路径能够随时变换。此外，利用 IP 规则、用户权限、用户域、用户口令等多重保护防止非法入侵。

10. 禁止不必要的服务

Windows Server 2003 系统中有许多不常用的服务自动处于激活状态，许多服务中可能存在的安全漏洞使攻击者甚至不需要账户就能控制计算机。为了系统的安全，应该关闭不常用的功能服务，从而大大减少安全风险。

选择【开始】|【设置】|【控制面板】命令，打开【控制面板】窗口，双击【管理工具】图标，打开【管理工具】窗口，双击【服务】图标，打开【服务】窗口，将不必要的服务进行禁止，如图 3.18 所示。

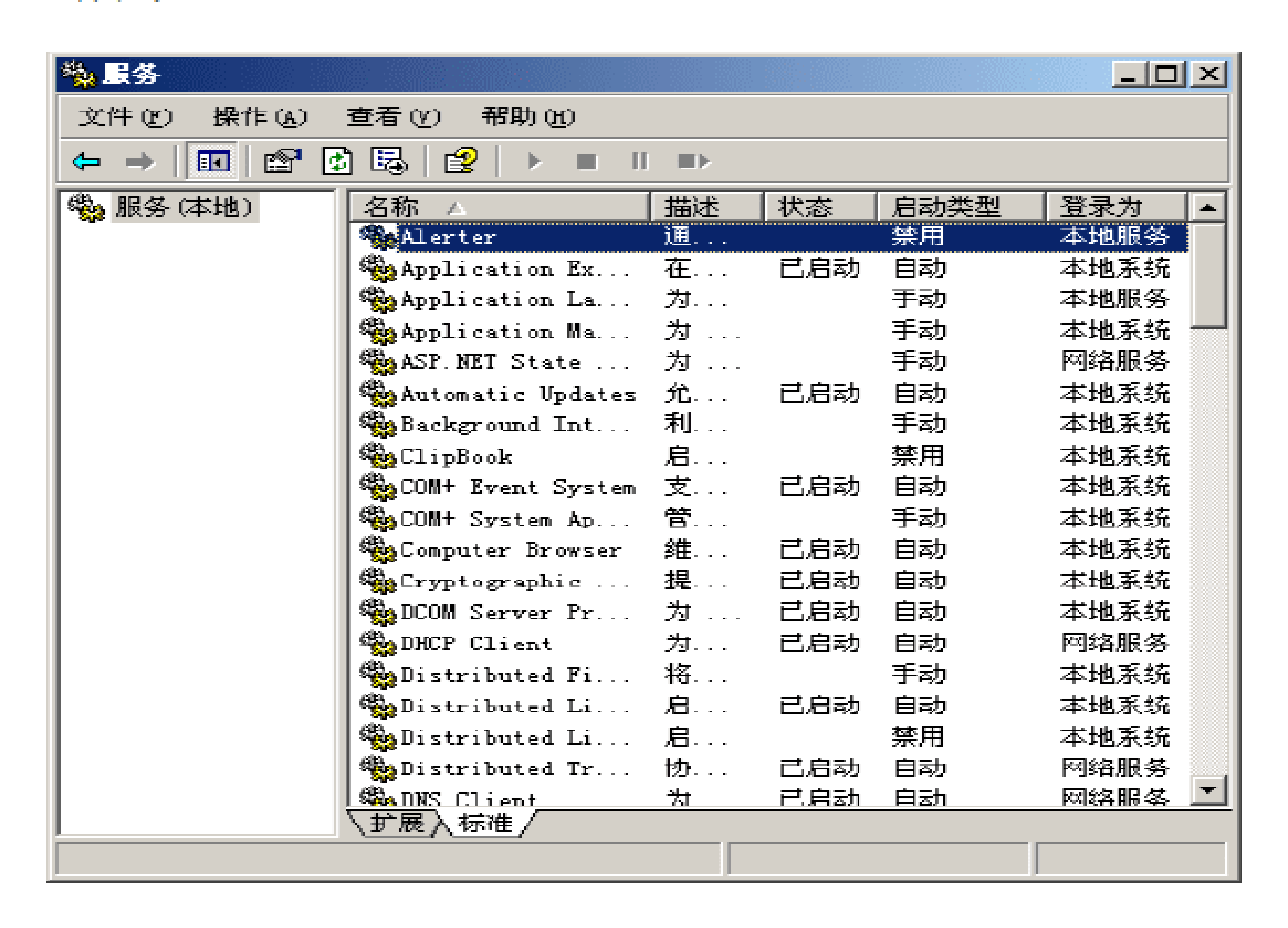


图 3.18　禁止不必要的服务

相关需要禁止的服务如下。

- Alerter：系统管理级警报。
- Application Management：提供软件安装服务，诸如分派、发布及删除等。
- ClipBook：支持【剪贴簿查看器】，从远程剪贴簿查阅剪贴页面。
- COM+ Event System：提供事件的自动发布及订阅 COM 组件。
- Computer Browser：维护网络计算机的最新列表，以及响应提供这个列表的请求。
- Distributed Link Tracking Client：当文件在网络域的 NTFS 卷中移动时发送通知。
- Distributed Transaction Coordinator：协调跨多个数据库、消息队列、文件系统等资源管理器的事务。
- Fax Service：发送和接收传真。
- FTP Publishing Service：通过 Internet 信息服务的管理单元提供 FTP 连接和管理。
- Indexing Service：本地和远程计算机上文件的索引内容和属性，并提供文件快速访问服务。
- Messenger：发送和接收系统管理员以及 Alerter 服务传递的消息。
- Net Logon：支持网络计算机 pass-through 账户登录身份验证事件。
- Network DDE：提供动态数据交换(DDE)的网络传输和安全特性服务。
- Network DDE DSDM：管理 DDE 共享动态数据交换。
- Network Monitor：网络监视器。
- NetMeeting Remote Desktop Sharing：允许有权限的用户使用 NetMeeting 远程访问



Windows 桌面。

- Plug and Play(在配置好所有硬件后应该禁止此服务)：管理设备安装及配置，并且通知程序关于设备更改的情况。
- Remote Procedure Call(RPC)：提供终节点映射程序(Endpoint Mapper)以及其他 RPC 服务。
- Remote Registry Service：允许远程注册表操作。
- Removable Storage：管理可移动媒体、驱动程序和库。
- Routing and Remote Access：在局域网以及广域网环境中为企业提供路由服务。
- Server：支持此计算机通过网络的文件、打印和命名管道共享。
- Smart Card：对插入在计算机智能卡阅读器中的智能卡进行管理和访问控制。
- Smart Card Helper：提供对连接到计算机上旧式智能卡的支持。
- Task Schedule：允许程序在指定时间的运行。
- TCP/IP NetBIOS Helper：提供 TCP/IP(NetBT)服务上的 NetBIOS 和网络上客户端的 NetBIOS 名称解析的支持。
- Telephone Service：提供 TAPI 支持，以便程序控制本地计算机、服务器以及 LAN 上的电话设备和基于 IP 的语音连接。
- Windows Management Instrumentation：提供系统管理信息。

3.3 Linux 网络操作系统的安全

随着 Internet 的日益普及，采用 Linux 操作系统作为服务器的用户也越来越多，这一方面是因为 Linux 是开放源代码的免费正版软件，另一方面也是因为 Linux 系统具有较好的稳定性和安全性。在使用 Linux 操作系统的时候，也要详细分析 Linux 系统的安全机制，找出它可能存在的安全隐患，给出相应的安全策略和保护措施是十分必要的。

3.3.1 Linux 网络操作系统的基本安全机制

Linux 网络操作系统提供了用户账号、文件系统权限和系统日志文件等基本安全机制，如果这些安全机制配置不当，就会使系统存在一定的安全隐患。

1. Linux 系统的用户账号

在 Linux 系统中，用户账号是用户身份的标志，它由用户名和用户口令两部分组成。在 Linux 系统中，系统将输入的用户名存放在/etc/passwd 文件中，而将输入的口令以加密的形式存放在/etc/shadow 文件中。在正常情况下，这些口令由操作系统保护，能够对其进行访问的只能是超级用户和操作系统的一些应用程序。但是如果配置不当，或者在系统运行出错的情况下，这些信息可能被普通用户非法获取。进而，不怀好意的用户就可以使用“口令破解”工具得到加密前的口令。

2. Linux 的文件系统权限

Linux 文件系统的安全主要是通过设置文件的权限来实现的。每一个 Linux 的文件或目

录都有 3 组属性，分别定义文件或目录的所有者、用户组和其他人的使用权限(只读、可写、可执行、允许 SUID、允许 SGID 等)，需要注意的是权限为 SGID 和 SUID 的可执行文件。SGID(SUID)中的 S 指 set，程序在运行时，其进程的 EUID(Effective User ID)或 EGID(Effective Group ID)会被设置成文件拥有者的 UIDGID，从而进程也具有了其 Owner 或 Owner Group 的权限。典型的应用是/bin/passwd 命令，其 Owner 是 root，权限是 4755。可以想象，如果使用不当，SGID 和 SUID 程序会给系统安全性带来极大的危害。某些入侵者暂时取得 root 权限后，往往会利用 SGID 或 SUID 程序为下次进入系统留下后门。为了防止这种情况发生，应当定期检查系统中的 SUID 和 SGID 程序。

3. 合理利用 Linux 的日志文件

Linux 的日志文件用来记录整个操作系统使用状况。作为一个 Linux 网络系统管理员要充分用好以下几个日志文件。

(1) /var/log/lastlog 文件。记录最后进入系统的用户信息，包括登录的时间、登录是否成功等。因此普通用户登录后只要用 lastlog 命令查看一下/var/log/lastlog 文件中记录账号的最后登录时间，再与自己的记录对比一下，就可以发现该账号是否被黑客盗用。

(2) /var/log/secure 文件。记录系统自开通以来所有用户的登录时间和地点，可以给系统管理员提供更多的参考。

(3) /var/log/wtmp 文件。记录当前和历史上登录到系统的用户的登录时间、地点和注销时间等信息。可以用 last 命令查看，若想清除系统登录信息，只需删除这个文件即可。

3.3.2 Linux 网络系统可能受到的攻击

Linux 操作系统是一种公开源代码的操作系统，因此比较容易受到来自底层的攻击，系统管理员一定要有安全防范意识，并对系统采取一定的安全措施，这样才能提高 Linux 系统的安全性。

对于系统管理员来说，特别是要搞清楚对 Linux 网络系统可能的攻击方法，并采取必要的措施保护自己的系统。对 Linux 服务器攻击的定义是，攻击是一种旨在妨碍、损害、削弱、破坏 Linux 服务器安全的未授权行为。攻击的范围可以从服务拒绝直至完全危害和破坏 Linux 服务器。

对 Linux 服务器攻击通常有 4 类。

1. “拒绝服务”攻击

“拒绝服务”攻击是指黑客采取具有破坏性的方法阻塞目标网络的资源，使网络暂时或永久瘫痪，从而使 Linux 网络服务器无法为正常的用户提供服务。例如，黑客可以利用伪造的源地址或受控的其他地方的多台计算机同时向目标计算机发出大量、连续的 TCP/IP 请求，从而使目标服务器系统瘫痪。

2. “口令破解”攻击

口令是保卫自己系统安全的第一道防线。“口令破解”攻击的目的是为了破解用户的口令，从而可以取得已经加密的信息资源。例如，黑客可以利用一台高速计算机，配合一个字典库，尝试各种口令组合，直到最终找到能够进入系统的口令，打开网络资源。



3. “欺骗用户”攻击

“欺骗用户”攻击是指网络黑客伪装成网络公司或计算机服务商的工程技术人员，向用户发出呼叫，并在适当的时候要求用户输入口令，这是用户最难对付的一种攻击方式，一旦用户口令失窃，黑客就可以利用该用户的账号进入系统。

4. “扫描程序和网络监听”攻击

许多网络入侵是从扫描开始的，利用扫描工具黑客能找出目标主机上各种各样的漏洞，并利用它对系统实施攻击。

网络监听也是黑客们常用的一种方法，当成功登录到一台网络上的主机，并取得了这台主机的超级用户控制权之后，黑客可以利用网络监听收集敏感数据或者认证信息，以便日后夺取网络中其他主机的控制权。

3.3.3 Linux 网络安全防范策略

Linux 是一个开放式系统，可以在网络上找到许多现成的程序和工具，这既方便了用户也方便了黑客，因为他们也能很容易地找到程序和工具来潜入 Linux 系统，或者盗取 Linux 系统上的重要信息。不过，只要仔细设定 Linux 的各种系统功能，并且加上必要的安全措施，就能让黑客们无机可乘。

1. 仔细设置每个内部用户的权限

为保护 Linux 网络系统的资源，在给内部网络用户开设账号时，要仔细设置每个内部用户的权限，一般应遵循“最小权限”原则，也就是仅给每个用户授予完成他们特定任务所必需的服务器访问权限。虽然这样做会大大加重系统管理员的管理工作量，但是为了整个网络系统的安全还是应该坚持遵守这个原则。

2. 确保用户口令文件/etc/shadow 的安全

对于网络系统而言，口令是比较容易出问题的地方，作为系统管理员应告诉用户在设置口令时要使用安全口令(在口令序列中使用非字母、非数字等特殊字符)并适当增加口令的长度(大于 6 个字符)。系统管理员要保护好/etc/passwd 和/etc/shadow 这两个文件的安全，不让无关人员获得这两个文件，这样黑客利用 John 等程序对/etc/passwd 和/etc/shadow 文件进行字典攻击以获取用户口令的企图就无法得逞。系统管理员要定期用 John 等程序对本系统的/etc/passwd 和/etc/shadow 文件进行模拟字典攻击，一旦发现有不安全的用户口令，要强制用户立即修改。

字典攻击：收集好密码可能包含的字符串，然后通过各种方式组合，即相当于从字典中查密码，逐一验证。

字典软件：这是一个可以自动编写密码的软件，它的功能是编写密码，是结合其他暴力破解软件的一种工具。 生成后可以利用流光等软件，是破解密码的一种方式，也就是猜密码，只不过用计算机来完成。比如有个密码要猜测，那就让计算机程序去逐个测试，拿什么去测试，就是字典了，在文件中录入一些字符，比如一个文件内容：1 2 3 4，那计算机就先从 1 开始到 4，如 12 13 14 等。



3. 加强对系统运行的监控和记录

Linux 网络系统管理员应对整个网络系统的运行状况进行监控和记录，这样通过分析记录数据，可以发现可疑的网络活动，并采取措施预先阻止今后可能发生的入侵行为。如果入侵行为已经实施，则可以利用记录数据跟踪和识别侵入系统的黑客。

4. 制订适当的数据备份计划

没有一种操作系统的运转是完全可靠的，也没有一种安全策略是万无一失的，因此作为 Linux 系统管理员，必须为系统制订适当的数据备份计划，充分利用磁带机、光盘刻录机、双机热备份等技术手段为系统保存数据备份，使系统一旦遭到破坏或黑客攻击而发生瘫痪时，能迅速恢复工作，把损失降到最小。

在完成 Linux 系统的安装以后应该对整个系统进行备份，以后可以根据这个备份来验证系统的完整性，从而发现系统文件是否被非法篡改过。如果发生系统文件已经被破坏的情况，也可以使用系统备份来恢复到正常的状态。

1)　CD-ROM 备份

当前最好的系统备份介质就是 CD-ROM 光盘，备份后可以定期将系统与光盘内容进行比较，以验证系统的完整性是否遭到破坏。如果对安全级别的要求特别高，还可以将光盘设置为可启动的并且将验证工作作为系统启动过程的一部分。这样只要可以通过光盘启动，就说明系统尚未被破坏过。

如果创建了一个只读的分区，那么可以定期从光盘映像重新装载它们。即使像/boot、/lib 和/sbin 这样不能被安装成只读的分区，仍然可以根据光盘映像来检查，甚至可以在启动时从另一个安全的映像重新下载它们。

2)　其他方式的备份

虽然/etc 中的许多文件经常会变化，但/etc 中的许多内容仍然可以放到光盘上用于系统完整性验证。其他不经常进行修改的文件，可以备份到另一个系统(如磁带)或压缩到一个只读目录中。这种办法可以在使用光盘映像进行验证的基础上再进行额外的系统完整性检查。

5. 保持最新的系统核心

由于 Linux 流通渠道很多，而且经常有更新的程序和系统补丁出现，因此，为了加强系统安全，一定要经常更新系统内核。

Kernel 是 Linux 操作系统的核心，它常驻内存，用于加载操作系统的其他部分，并实现操作系统的基本功能。由于 Kernel 控制计算机和网络的各种功能，因此，它的安全性对整个系统安全至关重要。在设定 Kernel 的功能时，只选择必要的功能，千万不要将所有功能照单全收，否则会使 Kernel 变得很大，既占用系统资源，也给黑客留下可乘之机。

在 Internet 上常常有最新的安全修补程序，Linux 系统管理员应该消息灵通，经常光顾安全新闻组，查阅新的修补程序。

6. 定期对 Linux 网络进行安全检查

Linux 网络系统的运转是动态变化的，因此对它的安全管理也是变化的，没有固定的模式可循，作为 Linux 网络系统的管理员，在为系统设置了安全防范策略后，应定期对系统



进行安全检查，并尝试对自己管理的服务器进行攻击，如果发现安全机制中的漏洞应立即采取补救措施，不给黑客以可乘之机。

3.3.4　加强 Linux 网络服务器的管理

可以采取以下措施，加强对 Linux 网络服务器的管理。

1. 记录对 Linux 系统的访问

Linux 系统管理员可以利用记录文件和记录工具记录事件，可以每天查看或扫描记录文件，这些文件记录了系统运行的所有信息。如果需要，还可以把高优先级的事件提取出来传送给相关人员处理，如果发现异常可以立即采取措施。

2. 取消不必要的服务

大多数 Linux 系统安装后，各种不同的服务都被激活，如 FTP、Telnet、UUCP、ntalk 等。多数情况下，其中有些服务很少会用到，让它们处于活动状态就像是把窗户打开让盗贼有机会溜进来一样。一般来说，除了 HTTP、SMTP、Telnet 和 FTP 之外，其他服务都应该取消，诸如简单文件传输协议(TFTP)、网络邮件存储及接收所用的 imap/ipop 传输协议、搜索资料用的 Gopher 以及用于时间同步的 Daytime 和 Time 等。

取消不必要服务的方法就是检查/etc/inetd.conf 文件，在不要的服务前加上“#”号，然后重启 inetd 后台程序，从而禁用它们。另外，一些服务(如数据库服务器)可能在开机过程中默认为启动，可以通过编辑/etc/rc.d/*目录等级禁用这些服务。许多有经验的管理员禁用了所有系统服务，只留下 SSH 通信端口。

3. 慎用 Telnet 服务

用 Telnet 进行远程登录时，用户名和用户密码是明文传输的，这就有可能被在网上监听的其他用户所截获。另一个危险是黑客可以利用 Telnet 登录系统，如果同时获取了超级用户密码，则对系统的危害将是灾难性的。因此，如果不是特别需要，不要开放 Telnet 服务。如果一定要开放 Telnet 服务，应该要求用户用特殊的工具软件进行远程登录，这样就可以在网上传送加密过的用户密码，以免密码在传输过程中被黑客截获。

还有一些报告系统状态的服务，如 Finger、Efinger、Systat 和 Netstat 等，虽然对系统查错和寻找用户非常有用，但也给黑客打开了方便之门。例如，黑客可以利用 Finger 服务查找用户的电话、使用目录及其他重要信息。因此，很多 Linux 系统将这些服务全部或部分取消，以增强系统的安全性。

Inetd 除了利用/etc/inetd.conf 设置系统服务项之外，还利用/etc/services 文件查找各项服务所使用的端口。因此，用户必须仔细检查该文件中各端口的设定，以免有安全漏洞。

在 Linux 中有两种不同的服务形态：一种是仅在有需要时才执行的服务，如 Finger 服务；另一种是一直在执行的永不停顿的服务。这类服务在系统启动时就开始执行，因此不能靠修改 Inetd 来停止其服务，而只能从修改/etc/rc.d/rc[n].d/文件或用 Run level editor 去修改它。提供文件服务的 NFS 服务器和提供 NNTP 新闻服务的 news 都属于这类服务，如果没有必要，最好取消这些服务。



4. 合理设置 NFS 服务和 NIS 服务

NFS(Network File System)服务允许工作站通过网络共享一个或多个服务器输出的文件。但对于配置不安全的 NFS 服务器来讲，用户不经登录就可以阅读或者更改存储在 NFS 服务器上的文件，使得 NFS 服务器很容易受到攻击。如果一定要提供 NFS 服务，要确保 NFS 服务器支持 Secure RPC(Secure Remote Procedure Call)，以便利用 DES(Data Encryption Standard)加密算法和指数密钥交换(Exponential Key Exchange)技术验证每个 NFS 请求的用户身份。

NIS(Network Information System)服务是一个分布式数据处理系统，它使网络中的计算机通过网络共享 passwd 文件、group 文件、主机表文件和其他共享的系统资源。NIS 服务也有漏洞，在 NIS 系统中，恶意用户可以利用自己编写的程序模仿 Linux 系统中的 ypserv 响应 ypbind 的请求，从而截获用户的密码。因此，NIS 的用户一定要使用 ypbind 的 secure 选项，并且不接受端口号小于 1024(非特权端口)的 ypserv 响应。

5. 小心配置 FTP 服务

FTP 服务的用户名和用户密码也是明文传输的。因此，为了系统的安全，必须禁止 root、bin、daemon、adm 等特殊用户对 FTP 服务器进行远程访问，限制某些主机不能连入 FTP 服务器，如果开放匿名 FTP 服务，则任何人都可以下载文件(有时还可以上传文件)，因此，除非特别需要一般应禁止匿名 FTP 服务。

6. 合理设置 POP-3 和 Sendmail 等电子邮件服务

对一般的 POP-3 服务来讲，电子邮件用户的口令是按明文方式传送到网络中的，黑客可以轻易截获用户名和用户密码。要想解决这个问题，必须安装支持加密传送密码的 POP-3 服务器(即支持 Authenticated POP 命令)，这样用户在往网络中传送密码之前，可以先对密码实施加密。

老版本的 Sendmail 邮件服务器程序存在安全隐患，为确保邮件服务器的安全，应尽可能安装已消除安全隐患的最新版的 Sendmail 服务器软件。

7. 加强对 WWW 服务器的管理，提供安全的 WWW 服务

当一个基于 Linux 系统的网站建立好之后，绝大部分用户是通过 Web 服务器，利用 WWW 浏览器对网络进行访问的，因此必须特别重视 Web 服务器的安全，无论采用哪种基于 HTTP 协议的 Web 服务器软件，都要特别关注 CGI(Common Gateway Interface)脚本。CGI 脚本是可执行程序，一般存放在 Web 服务器的 CGI-BIN 目录下面，在配置 Web 服务器时，要保证 CGI 可执行脚本只存放于 CGI-BIN 目录中。

8. 最好禁止提供 Finger 服务

在 Linux 系统下，使用 finger 命令，可以显示本地或远程系统中目前已登录用户的详细信息，黑客可以利用这些信息增大侵入系统的机会。为了系统的安全，最好禁止提供 Finger 服务，即从/usr/bin 下删除 finger 命令。如果要保留 Finger 服务，应将 Finger 文件更名，或修改权限为只允许 root 用户执行 finger 命令。



由于 Linux 操作系统使用广泛，又公开了源代码，因此是被广大计算机用户研究得最彻底的操作系统，而 Linux 本身的配置又相当复杂，按照前面的安全策略和保护机制，可以将系统的风险降到最低，但不可能彻底消除安全漏洞，作为 Linux 系统的管理员，一定要有安全防范意识，定期对系统进行安全检查，发现漏洞要立即采取措施，不给黑客以可乘之机。

复习思考题三

一、填空题

1. Windows NT 4 种域模型为单域模型、__________、多主域模型和__________模型。

2. 使用特殊技术对系统进行攻击，以便得到有针对性的信息就是一种__________攻击。

3. __________攻击是指通过向程序的缓冲区写入超出其长度的内容，从而破坏程序的堆栈，使程序转而执行其他的指令，以达到攻击的目的。

4. Windows NT 的安全管理主要包括__________、用户权限规则、__________和域管理机制等。

二、单项选择题

网络访问控制可分为自主访问控制和强制访问控制两大类。 ① 是指由系统对用户所创建的对象进行统一的限制性规定。 ② 是指由系统提供给用户有权对自身所创建的访问对象进行访问，并可将对这些对象的访问权授予其他用户和从授予权限的用户收回其访问权限。用户名/口令、权限安全、属性安全等都属于 ③ 。

(　　) ①　A. 服务器安全控制　　B. 检测和锁定控制
　　　　　C. 自主访问控制　　D. 强制访问控制

(　　) ②　A. 服务器安全控制　　B. 检测和锁定控制
　　　　　C. 自主访问控制　　D. 强制访问控制

(　　) ③　A. 服务器安全控制　　B. 检测和锁定控制
　　　　　C. 自主访问控制　　D. 强制访问控制

三、简答题

1. 简述漏洞的概念。
2. 漏洞对操作系统有什么影响？
3. 操作系统为什么会有安全问题？
4. 什么是访问控制？
5. Windows Server 2003 如何设置安全的密码？
6. Windows Server 2003 如何实现身份认证？
7. Linux 网络系统可能受到的攻击有哪些？
8. Linux 网络系统如何实现单一登录？

第 4 章　数据库与数据安全技术

学习目标

无论数据处于存储状态还是处于传输状态，都可能会受到安全威胁。要保证企事业单位的业务持续成功地运作，就要保护数据库系统中的数据安全。通过本章的学习，读者应掌握以下内容：

- 数据库系统特性及其安全。
- 数据库的安全特性。
- 数据库的安全保护。
- 数据的完整性。
- 数据备份和数据恢复。
- 数据容灾。

4.1　数据库安全概述

保证网络系统中数据安全的主要任务就是使数据免受各种因素的影响，保护数据的完整性、保密性和可用性。人为错误、硬盘损毁、计算机病毒、自然灾难等都有可能造成数据库中数据的丢失，给企事业单位造成无可估量的损失。例如，如果丢失了系统文件、客户资料、技术文档、人事档案文件、财务账目文件等，企事业单位的业务将难以正常进行。因此，所有的企事业单位管理者都应采取有效保护数据库的措施，使得灾难发生后，能够尽快地恢复系统中的数据，恢复系统的正常运行。

为了保护数据安全，可以采用很多安全技术和措施。这些技术和措施主要有数据完整性技术、数据备份和恢复技术、数据加密技术、访问控制技术、用户身份验证技术、数据的真伪鉴别技术和并发控制技术等。

4.1.1　数据库安全的概念

数据库安全是指数据库的任何部分都没有受到侵害，或没有受到未经授权的存取和修改。 数据库安全性问题一直是数据库管理员所关心的问题。

1. 数据库安全

数据库就是一种结构化的数据仓库。人们时刻都在和数据打交道，如存储在个人掌上计算机(PDA)中的数据、家庭预算的电子数据表格等。对于少量、简单的数据，如果与其他数据之间的关联较少或没有关联，则可将它们简单地存放在文件中。普通记录文件没有必要的结构来系统地反映数据间的复杂关系，也不能强制定义个别数据对象。但是企业数据都是相关联的，不可能使用普通的记录文件来管理大量的、复杂的系列数据，比如银行的客户数据或者生产厂商的生产控制数据等。



数据库安全主要包括数据库系统的安全性和数据库数据的安全性两层含义。

(1) 数据库系统的安全性。数据库系统的安全性是指在系统级控制数据库的存取和使用的机制，应尽可能地堵住潜在的各种漏洞，防止非法用户利用这些漏洞侵入数据库系统；保证数据库系统不因软、硬件故障及灾害的影响而不能正常运行。数据库系统安全包括：硬件运行安全；物理控制安全；操作系统安全；用户有连接数据库的授权；灾害、故障恢复。

(2) 数据库数据的安全性。数据库数据的安全性是指在对象级控制数据库的存取和使用的机制，哪些用户可存取指定的模式对象及在对象上允许有哪些操作类型。数据库数据安全包括：有效的用户名/口令鉴别；用户访问权限控制；数据存取权限、方式控制；审计跟踪；数据加密；防止电磁信息泄露。

数据库数据的安全措施应能确保数据库系统关闭后，当数据库数据存储媒体被破坏或当数据库用户误操作时，数据库数据信息不会丢失。对于数据库数据的安全性问题，数据库管理员可以采用系统双机热备份功能、数据库的备份和恢复、数据加密、访问控制等措施。

2. 数据库安全管理原则

一个强大的数据库安全系统应当确保其中信息的安全性，并对其进行有效的管理和控制。下面几项数据库管理规则有助于企业在安全规则中实现对数据库的安全保护。

1) 管理细分和委派原则

在数据库工作环境中，数据库管理员一般都是独立执行数据库的管理和其他事务工作，一旦出现岗位变换，将带来一连串的问题和效率低下。通过管理责任细分和任务委派，数据库管理员可从常规事务中解脱出来，把精力更多地放在解决数据库执行效率及与管理相关的重要问题上，从而保证任务的高效完成。企业应设法通过功能和可信赖的用户群进一步细分数据库管理的责任和角色。

2) 最小权限原则

企业必须本着“最小权限”原则，从需求和工作职能两方面严格限制对数据库的访问。通过角色的合理运用，“最小权限”可确保数据库功能限制和特定数据的访问。

3) 账号安全原则

对于每一个数据库连接来说，用户账号都是必需的。账号应遵循传统的用户账号管理方法来进行安全管理，这包括密码的设定和更改、账号锁定功能、对数据提供有限的访问权限、禁止休眠状态的账户、账户的生命周期等。

4) 有效审计原则

数据库审计是数据库安全的基本要求，它可用来监视各用户对数据库施加的操作。企业应针对自己的应用和数据库活动定义审计策略。条件允许的地方可采取智能审计，这样不仅能节约时间，而且能减少执行审计的范围和对象。通过智能限制日志大小，还能突出更加关键的安全事件。



4.1.2 数据库管理系统及特性

1. 数据库管理系统简介

数据库管理系统(DBMS)已经发展了近 20 年。人们提出了许多数据模型，并一一得以实现，其中比较重要的是关系模型。在关系型数据库中，数据项保存在行中，文件就像是一个表。关系被描述成不同数据表间的匹配关系。区别关系模型和网络及分级型数据库重要的一点就是数据项关系可以被动态地描述或定义，而不需要因结构改变而重新加载数据库。

早在 1980 年，数据库市场就被关系型数据库管理系统所占领。这个模型基于一个可靠的基础，可以简单并恰当地将数据项描述成为表(Table)中的记录行(Raw)。关系模型第一次广泛地推行是在 1980 年，由于当时一种标准的数据库访问程序语言被开发，这种语言被称作结构化查询语言(SQL)。今天，成千上万使用关系型数据库的应用程序已经被开发出来，如跟踪客户端处理的银行系统、仓库货物管理系统、客户关系管理(CRM)系统和人力资源管理系统等。由于数据库保证了数据的完整性，企业通常将他们的关键业务数据存放在数据库中。因此保护数据库安全、避免错误和防止数据库故障已经成为企业所关注的重点。

2. 数据库管理系统的安全功能

DBMS 是专门负责数据库管理和维护的计算机软件系统。它是数据库系统的核心，不仅负责数据库的维护工作，还能保护数据库的安全性和完整性。

DBMS 是近似于文件系统的软件系统，通过它应用程序和用户可以取得所需的数据。然而，与文件系统不同，DBMS 定义了所管理的数据之间的结构和约束关系，且提供了一些基本的数据管理和安全功能。

1) 数据的安全性

在网络应用上，数据库必须是一个可以存储数据的安全地方。DBMS 能够提供有效的备份和恢复功能，来确保在故障和错误发生后，数据能够尽快地恢复并被应用所访问。对于一个企事业单位来说，把关键的和重要的数据存放在数据库中，这就要求 DBMS 必须能够防止未授权的数据访问。

只有数据库管理员对数据库中的数据拥有完全的操作权限，并可以规定各用户的权限，DBMS 保证对数据的存取方法是唯一的。每当用户想要存取敏感数据时，DBMS 就进行安全性检查。在数据库中，对数据进行各种类型的操作(检索、修改、删除等)时，DBMS 都可以对其实施不同的安全检查。

2) 数据的共享性

一个数据库中的数据不仅可以为同一企业或组织内部的各个部门所共享，也可为不同组织、不同地区甚至不同国家的多个应用和用户同时进行访问，而且还要不影响数据的安全性和完整性，这就是数据共享。数据共享是数据库系统的目的，也是它的一个重要特点。

数据库中数据的共享主要体现在以下几个方面。

(1) 不同的应用程序可以使用同一个数据库。

(2) 不同的应用程序可以在同一时刻去存取同一个数据。

(3) 数据库中的数据不但可供现有的应用程序共享，还可为新开发的应用程序使用。



(4) 应用程序可用不同的程序设计语言编写，它们可以访问同一个数据库。

3) 数据的结构化

基于文件的数据的主要优势就在于它利用了数据结构。数据库中的文件相互联系，并在整体上服从一定的结构形式。数据库具有复杂的结构，不仅是因为它拥有大量的数据，同时也因为在数据之间和文件之间存在着种种联系。数据库的结构使开发者避免了针对每一个应用都需要重新定义数据逻辑关系的过程。

4) 数据的独立性

数据的独立性就是数据与应用程序之间不存在相互依赖关系，也就是数据的逻辑结构、存储结构和存取方法等不因应用程序的修改而改变；反之亦然。从某种意义上讲，一个DBMS 存在的理由就是为了在数据组织和用户的应用之间提供某种程度的独立性。数据库系统的数据独立性可分为物理独立性和逻辑独立性两个方面。

(1) 物理独立性。数据库物理结构的变化不影响数据库的应用结构，从而也就不影响其相应的应用程序。这里的物理结构是指数据库的物理位置、物理设备等。

(2) 逻辑独立性。数据库逻辑结构的变化不影响用户的应用程序，修改或增加数据类型、改变各表之间的联系等都不会导致应用程序的修改。

以上两种数据独立性都要依靠于 DBMS 来实现。到目前为止，物理独立性已经实现，但逻辑独立性实现起来非常困难。因为数据结构一旦发生变化，一般情况下，相应的应用程序都要进行或多或少的修改。

5) 其他安全功能

DBMS 除了具有一些基本的数据库管理功能外，在安全性方面，它还具有以下功能。

(1) 保证数据的完整性，抵御一定程度的物理破坏，能维护和提交数据库内容。

(2) 实施并发控制，避免数据的不一致性。

(3) 数据库的数据备份与数据恢复。

(4) 能识别用户、分配授权和进行访问控制，包括用户的身份识别和验证。

3. 数据库事务

“事务”是数据库中的一个重要概念，是一系列操作过程的集合，也是数据库数据操作的并发控制单位。一个“事务”就是一次活动所引起的一系列的数据库操作。例如，一个会计“事务”可能是由读取借方数据、减去借方记录中的借款数量、重写借方记录、读取贷方记录、在贷方记录的数量加上从借方扣除的数量、重写贷方记录、写一条单独的记录来描述这次操作以便日后审计等操作组成。所有这些操作组成了一个“事务”，描述了一个业务动作。无论借方的动作还是贷方的动作，哪一个没有被执行，数据库都不会反映该业务执行的正确性。

DBMS 在数据库操作时对“事务”进行定义，要么一个“事务”应用的全部操作结果都反映在数据库中(全部完成)，要么就一点都没有反映在数据库中(全部撤除)，数据库回到该次事务操作的初始状态。这就是说，一个数据库“事务”序列中的所有操作只有两种结果：全部执行和全部撤除。因此，“事务”是不可分割的单位。

上述会计“事务”例子包含了两个数据库操作：从借方数据中扣除资金；在贷方记录中加入这部分资金。如果系统在执行该“事务”的过程中崩溃，而此时已修改完毕借方数

据，但还没有修改贷方数据，资金就会在此时物化。如果把这两个步骤合并成一个事务命令，这在数据库系统执行时，要么全部完成，要么一点都不完成。当只完成一部分时，系统是不会对已做的操作予以响应的。

4.1.3　数据库系统的缺陷和威胁

大多数企业、组织及政府部门的电子数据都保存在各种数据库中。他们用这些数据库保存一些敏感信息，比如员工薪水、医疗记录、员工个人资料等。数据库服务器还掌握着敏感的金融数据，包括交易记录、商业事务和账号数据，战略上的或者专业的信息，比如专利和工程数据、甚至市场计划等应该保护起来防止竞争者和其他非法者获取的资料。

1. 数据库系统的缺陷

常见的数据库的安全漏洞和缺陷有以下几种。

(1)　数据库应用程序通常都同操作系统的最高管理员密切相关，如 Oracle、Sybase 和 SQL Server 数据库系统都涉及用户账号和密码、认证系统、授权模块和数据对象的许可控制、内置命令(存储过程)、特定的脚本和程序语言、中间件、网络协议、补丁和服务包、数据库管理和开发工具等。许多数据库系统管理员都把全部精力投入到管理这些复杂的系统中。安全漏洞和不当的配置通常会造成严重的后果，且都难以发现。

(2)　人们对数据库安全的忽视。人们认为只要把网络和操作系统的安全搞好了，所有的应用程序也就安全了。现在的数据库系统都有很多方面被误用或者有漏洞影响到安全。而且常用的关系型数据库都是“端口”型的，这就表示任何人都能够绕过操作系统的安全机制，利用分析工具连接到数据库上。

(3)　部分数据库机制威胁网络低层安全。例如，某公司的数据库里面保存着所有技术文档、手册和白皮书，但却不重视数据库的安全。这样，即使运行在一个非常安全的操作系统上，入侵者也能很容易通过数据库获得操作系统权限。这些存储过程能提供一些执行操作系统命令的接口，而且能访问所有的系统资源，如果该数据库服务器还同其他服务器建立着信任关系，那么，入侵者就能够对整个域产生严重的安全威胁。因此，少数数据库安全漏洞不仅威胁数据库的安全，也威胁到操作系统和其他可信任系统的安全。

(4)　安全特性缺陷。大多数关系型数据库已经存在 10 多年了，都是成熟的产品。但 IT 业界和安全专家对网络和操作系统要求的许多安全特性在多数关系数据库上还没有被使用。

(5)　数据库账号密码容易泄露。多数数据库提供的基本安全特性，都没有相应机制来限制用户必须选择健壮的密码。许多系统密码都能给入侵者访问数据库的机会，更有甚者，有些密码就储存在操作系统的普通文本文件中。比如 Oracle 内部密码，储存在 strxxx. crud 文件中，其中 xxx 是 Oracle 系统 ID 和 SID 号。该密码用于数据库启动进程，提供完全访问数据库资源功能，该文件在 Windows NT 中需要设置权限。Oracle 监听进程密码保存在文件 listener.ora 中，入侵者可以通过这个弱点进行 DoS 攻击。

(6)　操作系统后门。多数数据库系统都有一些特性，来满足数据库管理员的需要，这些也成为数据库主机操作系统的后门。

(7)　木马的威胁。著名的木马能够在密码改变存储过程时修改密码，并能告知入侵者。



比如，可以添加几行信息到 sp_password 中，记录新账号到库表中，通过 E-mail 发送这个密码，或者写到文件中以后使用等。

2. 数据库系统的威胁形式

对数据库构成的威胁主要有篡改、损坏和窃取 3 种表现形式。

(1) 篡改。篡改指的是对数据库中的数据未经授权进行的修改，使其失去原来的真实性。篡改的形式具有多样性，但有一点是明确的，就是在造成影响之前很难发现它。篡改是由于人为因素产生的。一般来说，发生这种人为威胁的原因主要有个人利益驱动、隐藏证据、恶作剧和无知等。

(2) 损坏。网络系统中数据的损坏是数据库安全性所面临的一个威胁。其表现形式是表和整个数据库部分或全部被删除、移走或破坏。产生这种威胁的原因主要有破坏、恶作剧和病毒。破坏往往都带有明确的作案动机；恶作剧者往往是出于爱好或好奇而给数据库造成损坏；计算机病毒不仅对系统文件进行破坏，也对数据文件进行破坏。

(3) 窃取。窃取一般是针对敏感数据进行的。窃取的手法除了将数据复制到软盘之类的可移动介质上外，还可以把数据打印后取走。导致窃取威胁的因素有工商业间谍、不满和要离开的员工、被窃的数据可能比想象中的更有价值等。

3. 数据库系统威胁的来源

数据库安全的威胁主要来自以下几个方面。

(1) 物理和环境的因素。如物理设备的损坏、设备的机械和电气故障、火灾、水灾以及磁盘磁带丢失等。

(2) 事务内部故障。数据库“事务”是指数据操作的并发控制单位，是一个不可分割的操作序列。数据库事务内部的故障多发生于数据的不一致性，主要表现有丢失修改、不能重复读、无用数据的读出。

(3) 系统故障。系统故障又叫软故障，是指系统突然停止运行时造成的数据库故障。这些故障不破坏数据库，但影响正在运行的所有事务，因为缓冲区中的内容会全部丢失，运行的事务将非正常终止，从而造成数据库处于一种不正确的状态。

(4) 介质故障。介质故障又称硬故障，主要指外存储器故障，如磁盘磁头碰撞、瞬时的强磁场干扰等。这类故障会破坏数据库或部分数据库，并影响正在使用数据库的所有事务。

(5) 并发事件。在数据库实现多用户共享数据时，可能由于多个用户同时对一组数据的不同访问而使数据出现不一致现象。

(6) 人为破坏。某些人为了某种目的，故意破坏数据库。

(7) 病毒与黑客。病毒可破坏计算机中的数据，使计算机处于不正确或瘫痪状态；黑客是一些精通计算机网络和软、硬件的计算机操作者，他们往往利用非法手段取得相关授权，非法地读取甚至修改其他计算机数据。黑客的攻击和系统病毒发作可破坏数据保密性和数据完整性。

(8) 未经授权非法访问或非法修改数据库的信息，窃取数据库数据或使数据失去真实性。

(9) 对数据不正确的访问引起数据库中数据的错误。

(10) 网络及数据库的安全级别不能满足应用的要求。

(11) 网络和数据库的设置错误和管理混乱造成越权访问和越权使用数据。

4.2　数据库的安全特性

为了保证数据库数据的安全可靠和正确有效，DBMS 必须提供统一的数据保护功能。数据保护也称为数据控制，主要包括数据库的安全性、完整性、并发控制和恢复。下面以多用户数据库系统 Oracle 为例，阐述数据库的安全特性。

4.2.1　数据库的安全性

数据库的安全性是指保护数据库以防止不合法的使用所造成的数据泄露、更改或破坏。在数据库系统中有大量的计算机系统数据集中存放，为许多用户所共享，这样就使安全问题更为突出。在一般的计算机系统中，安全措施是一级一级设置的。

1. 数据库的存取控制

在数据库存储一级可采用密码技术，若物理存储设备失窃，它能起到保密作用。在数据库系统中可提供数据存取控制，来实施该级的数据保护。

1)　数据库的安全机制

多用户数据库系统(如 Oracle)提供的安全机制可做到：

(1)　防止非授权的数据库存取。

(2)　防止非授权的对模式对象的存取。

(3)　控制磁盘使用。

(4)　控制系统资源使用。

(5)　审计用户动作。

在 Oracle 服务器上提供了一种任意存取控制，它是一种基于特权限制信息存取的方法。用户要存取某一对象必须有相应的特权授予该用户。已授权的用户可任意地授权给其他用户。

Oracle 保护信息的方法采用任意存取控制来限制全部用户对命名对象的存取。用户对对象的存取受特权控制，一种特权是存取一个命名对象的许可，为一种规定格式。

2)　模式和用户机制

Oracle 使用多种不同的机制管理数据库安全性，其中有模式和用户两种机制。

(1)　模式机制。模式为模式对象的集合，模式对象如表、视图、过程和包等。

(2)　用户机制。每一个 Oracle 数据库有一组合法的用户，可运行一个数据库应用和使用该用户连接到定义该用户的数据库。当建立一个数据库用户时，对该用户建立一个相应的模式，模式名与用户名相同。一旦用户连接一个数据库，该用户就可存取相应模式中的全部对象，一个用户仅与同名的模式相联系，所以用户和模式是类似的。



2. 特权和角色

1) 特权

特权是执行一种特殊类型的 SQL 语句或存取另一用户对象的权力，有系统特权和对象特权两类。

(1) 系统特权。系统特权是执行一种特殊动作或者在对象类型上执行一种特殊动作的权力。系统特权可授权给用户或角色。系统可将授予用户的系统特权授给其他用户或角色，同样，系统也可从那些被授权的用户或角色处收回系统特权。

(2) 对象特权。对象特权是指在表、视图、序列、过程、函数或包上执行特殊动作的权利。对于不同类型的对象，有不同类型的对象特权。

2) 角色

角色是相关特权的命名组。数据库系统利用角色可更容易地进行特权管理。

(1) 角色管理的优点。

① 减少特权管理。

② 动态特权管理。

③ 特权的选择可用性。

④ 应用可知性。

⑤ 专门的应用安全性。

一般地，建立角色有两个目的：一是为数据库应用管理特权；二是为用户组管理特权。相应的角色分别称为应用角色和用户角色。

① 应用角色是系统授予的运行一组数据库应用所需的全部特权。一个应用角色可授予其他角色或指定用户。一个应用可有几种不同角色，具有不同特权组的每一个角色在使用应用时可进行不同的数据存取。

② 用户角色是为具有公开特权需求的一组数据库用户而建立的。

(2) 数据库角色的功能。

① 一个角色可被授予系统特权或对象特权。

② 一个角色可授权给其他角色，但不能循环授权。

③ 任何角色可授权给任何数据库用户。

④ 授权给一个用户的每一角色可以是可用的，也可是不可用的。

⑤ 一个间接授权角色(授权给另一角色的角色)对一个用户可明确其可用或不可用。

⑥ 在一个数据库中，每一个角色名是唯一的。

3. 审计

审计是对选定的用户动作的监控和记录，通常用于审查可疑的活动、监视和收集关于指定数据库活动的数据。

1) Oracle 支持的 3 种审计类型

(1) 语句审计。语句审计是指对某种类型的 SQL 语句进行的审计，不涉及具体的对象。这种审计既可对系统的所有用户进行，也可对部分用户进行。

(2) 特权审计。特权审计是指对执行相应动作的系统特权进行的审计，不涉及具体对象。这种审计也是既可对系统的所有用户进行，也可对部分用户进行。

(3) 对象审计。对象审计是指对特殊模式对象的访问情况的审计，不涉及具体用户，是监控有对象特权的 SQL 语句。

2) Oracle 允许的审计选择范围

(1) 审计语句的成功执行、不成功执行，或其两者都包括。

(2) 对每一用户会话审计语句的执行审计一次或对语句的每次执行审计一次。

(3) 审计全部用户或指定用户的活动。

当数据库的审计是可能时，在语句执行阶段产生审计记录。审计记录包含有审计的操作、用户执行的操作、操作的日期和时间等信息。审计记录可存放于数据字典表(称为审计记录)或操作系统审计记录中。

4.2.2 数据库的完整性

数据库的完整性是指保护数据库数据的正确性和一致性。它反映了现实中实体的本来面貌。数据库系统要提供保护数据完整性的功能。系统用一定的机制检查数据库中的数据是否满足完整性约束条件。Oracle 应用于关系型数据库的表的数据完整性有下列类型。

(1) 空与非空规则。在插入或修改表的行时允许或不允许包含有空值的列。

(2) 唯一列值规则。允许插入或修改表的行在该列上的值唯一。

(3) 引用完整性规则。

(4) 用户定义规则。

Oracle 允许定义和实施每一种类型的数据完整性规则，如空与非空规则、唯一列值规则和引用完整性规则等，这些规则可用完整性约束和数据库触发器来定义。

1. 完整性约束

1) 完整性约束条件

完整性约束条件是作为模式的一部分，对表的列定义的一些规则的说明性方法。具有定义数据完整性约束条件功能和检查数据完整性约束条件方法的数据库系统可实现对数据库完整性的约束。

完整性约束有数值类型与值域的完整性约束、关键字的约束、数据联系(结构)的约束等。这些约束都是在稳定状态下必须满足的条件，叫静态约束。相应地，还有动态约束，指数据库中的数据从一种状态变为另一种状态时，新旧数值之间的约束，如更新人的年龄时新值不能小于旧值等。

2) 完整性约束的优点

利用完整性约束实施数据完整性规则具有以下优点。

(1) 定义或更改表时，不需要程序设计便可很容易地编写程序并可消除程序性错误，其功能由 Oracle 控制。

(2) 对表所定义的完整性约束被存储在数据字典中，所以由任何应用进入的数据都必须遵守与表相关联的完整性约束。

(3) 具有最大的开发能力。当由完整性约束所实施的事务规则改变时，管理员只需改变完整性约束的定义，所有应用自动地遵守所修改的约束。

(4) 完整性约束存储在数据字典中，数据库应用可利用这些信息，在 SQL 语句执行之



前或 Oracle 检查之前，就可立即反馈信息。

(5) 完整性约束说明的语义被清楚地定义，对于每一指定的说明规则可实现性能优化。

(6) 完整性约束可临时地使其不可用，使之在装入大量数据时避免约束检索的开销。当数据库装入完成时，完整性约束可容易地使其可用，任何破坏完整性约束的新记录都可在另外的表中列出。

2. 数据库触发器

1) 触发器的定义

数据库触发器是使用非说明方法实施的数据单元操作过程。利用数据库触发器可定义和实施任何类型的完整性规则。

Oracle 允许定义过程，当对相关的表进行 insert、update 或 delete 语句操作时，这些过程被隐式地执行，这些过程就称为数据库触发器。触发器类似于存储过程，可包含 SQL 语句和 PL/SQL 语句，并可调用其他的存储过程。过程与触发器的差别在于其调用方法：过程由用户或应用显式地执行；而触发器是为一个激发语句(insert、update、delete)发出而由 Oracle 隐式地触发。一个数据库应用可隐式地触发存储在数据库中的多个触发器。

2) 触发器的组成

一个触发器由 3 部分组成：触发事件或语句、触发限制和触发器动作。触发事件或语句是指引起激发触发器的 SQL 语句，可为对一个指定表的 insert、update 或 delete 语句。触发限制是指定一个布尔表达式，当触发器激发时该布尔表达式必须为真。触发器作为过程，是 PL/SQL 块，当触发语句发出、触发限制计算为真时该过程被执行。

3) 触发器的功能

在许多情况下触发器补充了 Oracle 的标准功能，以提供高度专用的数据库管理系统。一般触发器用于实现以下目的：

(1) 自动地生成导出列值。

(2) 实施复杂的安全审核。

(3) 在分布式数据库中实施跨节点的完整性引用。

(4) 实施复杂的事务规则。

(5) 提供透明的事件记录。

(6) 提供高级的审计。

(7) 收集表存取的统计信息。

4.2.3 数据库的并发控制

数据库是一种共享资源库，可为多个应用程序所共享。在许多情况下，由于应用程序涉及的数据量可能很大，常常会涉及输入/输出的交换。为了有效地利用数据库资源，可能多个程序或一个程序的多个进程并行地运行，这就是数据库的并发操作。

在多用户数据库环境中，多个用户程序可并行地存取数据。并发控制是指在多用户的环境下，对数据库的并行操作进行规范的机制，其目的是为了避免数据的丢失修改、无效数据的读出与不可重复读数据等，从而保证数据的正确性与一致性。并发控制在多用户的模式下是十分重要的，但这一点经常被一些数据库应用人员所忽视，而且因为并发控制的



层次和类型非常丰富和复杂，有时使人难以抉择，不清楚如何衡量并发控制的原则和途径。

1. 一致性和实时性

一致性的数据库就是指并发数据处理响应过程已完成的数据库。例如，一个会计数据库，当它的借方记录与相应的贷方记录相匹配的情况下，它就是数据一致的。

一个实时的数据库就是指所有的事务全部执行完毕后才响应。如果一个正在运行数据库管理的系统出现了故障而不能继续进行数据处理，原来事务的处理结果还存储在缓存中而没有写入磁盘文件中，当系统重新启动时，系统数据就是非实时性的。

数据库日志用来在故障发生后恢复数据库时保证数据库的一致性和实时性。

2. 数据的不一致现象

事务并发控制不当，可能会产生丢失修改、读无效数据、不可重复读等数据不一致现象。

1)　丢失修改

丢失数据是指一个事务的修改覆盖了另一个事务的修改，使前一个修改丢失。比如两个事务 T_1 和 T_2 读入同一数据，T_2 提交的结果破坏了 T_1 提交的数据，使 T_1 对数据库的修改丢失，造成数据库中的数据错误。

2)　读无效数据

无效数据的读出是指不正确数据的读出。比如事务 T_1 将某一值修改，然后事务 T_2 读该值，此后 T_1 由于某种原因撤销对该值的修改，这样就造成 T_2 读取的数据是无效的。

3)　不可重复读

在一个事务范围内，两个相同的查询却返回了不同数据，这是由于查询时系统中其他事务修改的提交而引起的。比如事务 T_1 读取某一数据，事务 T_2 读取并修改了该数据，T_1 为了对读取值进行检验而再次读取该数据，便得到不同的结果。

但在应用中为了提高并发度，可以容忍一些不一致现象。例如，大多数业务经适当调整后可以容忍不可重复读。当今流行的关系数据库系统(如 Oracle、SQL Server 等)是通过事务隔离与封锁机制来定义并发控制所要达到的目标的，根据其提供的协议，可以得到几乎任何类型的合理的并发控制方式。

并发控制数据库中的数据资源必须具有共享属性。为了充分利用数据库资源，应允许多个用户并行操作数据库。数据库必须能对这种并行操作进行控制，以保证数据在不同的用户使用时的一致性。

3. 并发控制的实现

并发控制的实现途径有多种，如果 DBMS 支持，当然最好是运用其自身的并发控制能力。如果系统不能提供这样的功能，可以借助开发工具的支持，还可以考虑调整数据库应用程序，有的时候可以通过调整工作模式来避开这种会影响效率的并发操作。

并发控制能力是指多用户在同一时间对相同数据同时访问的能力。一般的关系型数据库都具有并发控制能力，但是这种并发功能也会对数据的一致性带来危险。试想，若有两个用户都试图访问某个银行用户的记录，并同时要求修改该用户的存款余额时，情况将会怎样呢?



4.2.4 数据库的恢复

当使用一个数据库时，总希望数据库的内容是可靠的、正确的，但由于计算机系统的故障(硬件故障、软件故障、网络故障、进程故障和系统故障等)影响数据库系统的操作，影响数据库中数据的正确性，甚至破坏数据库，使数据库中数据全部或部分丢失。因此当发生上述故障后，希望能尽快恢复到原数据库状态或重新建立一个完整的数据库，该处理称为数据库恢复。数据库恢复子系统是数据库管理系统的一个重要组成部分。具体的恢复处理因所发生的故障类型所影响的情况和结果而变化。

1. 操作系统备份

不管为 Oracle 数据库设计什么样的恢复模式，数据库的数据文件、日志文件和控制文件的操作系统备份都是绝对需要的，它是保护介质故障的策略。操作系统备份分为完全备份和部分备份。

1) 完全备份

完全备份将构成 Oracle 数据库的全部数据库文件、在线日志文件和控制文件的一个操作系统备份。一个完全备份在数据库正常关闭后进行，不能在实例故障后进行。此时，所有构成数据库的全部文件是关闭的，并与当前状态相一致。在数据库打开时不能进行完全备份。由完全备份得到的数据库文件在任何类型的介质恢复模式中都是有用的。

2) 部分备份

部分备份是除完全备份以外的任何操作系统的备份，可在数据库打开或关闭状态下进行。如单个表空间中全部数据文件的备份、单个数据文件的备份和控制文件的备份。部分备份仅对在归档日志方式下运行数据库有用，数据文件可由部分备份恢复，在恢复过程中与数据库其他部分一致。

通过正规备份，并且快速地将备份介质运送到安全的地方，数据库就能够在大多数的灾难中得到恢复。恢复文件的使用是从一个基点的数据库映像开始，到一些综合的备份和日志。由于不可预知的物理灾难，一个完全的数据库恢复(重应用日志)可以使数据库映像恢复到尽可能接近灾难发生的时间点的状态。对于逻辑灾难，如人为破坏或者应用故障等，数据库映像应该恢复到错误发生前的那一点。

在一个数据库的完全恢复过程中，基点后所有日志中的事务被重新应用，所以结果就是一个数据库映像反映所有在灾难前已接受的事务，而没有被接受的事务则不被反映。数据库恢复可以恢复到错误发生前的最后一个时刻。

2. 介质故障的恢复

介质故障是当一个文件、文件的一部分或一块磁盘不能读或不能写时出现的故障。介质故障的恢复有以下两种形式，由数据库运行的归档方式决定。

(1) 如果数据库是可运行的，它的在线日志仅可重用但不能归档，此时介质恢复可使用最新的完全备份的简单恢复。

(2) 如果数据库可运行且其在线日志是可归档的，该介质故障的恢复是一个实际恢复过程，需重构受损的数据库，恢复到介质故障前的一个指定事务状态。

不管采用哪种方式，介质故障的恢复总是将整个数据库恢复到故障前的一个事务状态。如果数据库是在归档日志方式下运行，可采用完全介质恢复和不完全介质恢复两种方式进行。

1)　完全介质恢复

完全介质恢复可恢复全部丢失的修改。仅当所有必要的日志可用时才可能这样做。可使用不同类型的完全介质恢复，这要取决于损坏的文件和数据库的可用性。

(1)　关闭数据库的恢复。当数据库可被装配但是关闭时，如完全不能正常使用，此时可进行全部的或单个损坏数据文件的完全介质恢复。

(2)　打开数据库的离线表空间的恢复。当数据库是打开状态时，完全介质恢复可以处理。未损坏的数据库表空间在线时可以使用，而当受损空间离线时，其所有数据文件可作为完全介质恢复的单位。

(3)　打开数据库的离线表空间的单个数据文件的恢复。当数据库是打开状态时，完全介质恢复可以对其处理。未损坏的数据库表空间处于在线状态时，也可以使用完全介质恢复，而受损的表空间处于离线状态时，该表空间指定的单个受损数据文件可被恢复。

(4)　使用备份控制文件的恢复。当控制文件的所有复制由于磁盘故障而受损时，可使用备份控制文件进行完全介质恢复而不丢失数据。

2)　不完全介质恢复

不完全介质恢复是在完全介质恢复不可能或不要求时进行的介质恢复。可使用不同类型的不完全介质恢复，重构受损的数据库，使其恢复到介质故障前或用户出错前事务的一致性状态。根据具体受损数据的不同，可采用不同的不完全介质恢复。

(1)　基于撤销的不完全介质恢复。在某种情况下，不完全介质恢复必须被控制，数据库管理员可撤销在指定点的操作。可在一个或多个日志组(在线的或归档的)已被介质故障所破坏，不能用于恢复过程时使用基于撤销的恢复。介质恢复必须控制，在使用最近的、未受损的日志组于数据文件后中止恢复操作。

(2)　基于时间和修改的恢复。如果数据库管理员希望恢复到过去的某个指定点，不完全介质恢复是理想的。当用户意外地删除一个表，并注意到错误提交的估计时间，数据库管理员可立即关闭数据库，利用基于时间的恢复，恢复到用户错误之前时刻。当出现系统故障而使一个在线日志文件的部分被破坏时，所有活动的日志文件突然不能使用，实例被中止，此时需要利用基于修改的介质恢复。在这两种恢复情况下，不完全介质恢复的终点可由时间点或系统修改号(SCN)来指定。

4.3　数据库的安全保护

目前，计算机大批量数据存储的安全问题、敏感数据的防窃取和防篡改问题越来越引起人们的重视。数据库系统作为计算机信息系统的核心部件，数据库文件作为信息的聚集体，其安全性是非常重要的。因此，对数据库数据和文件进行安全保护是非常必要的。

4.3.1　数据库的安全保护层次

数据库系统的安全除依赖于其内部的安全机制外，还与外部网络环境、应用环境、从



业人员素质等因素有关，因此，从广义上讲，数据库系统的安全框架可以划分为以下 3 个层次。

(1) 网络系统层次。

(2) 操作系统层次。

(3) 数据库管理系统层次。

这 3 个层次构成数据库系统的安全体系，与数据库安全的关系是逐层紧密联系的，防范的重要性也逐层加强，从外到内、由表及里保证数据的安全。

1. 网络系统层次安全

从广义上讲，数据库的安全首先依赖于网络系统。随着 Internet 的发展和普及，越来越多的公司将其核心业务向互联网转移，各种基于网络的数据库应用系统纷纷涌现出来，面向网络用户提供各种信息服务。可以说，网络系统是数据库应用的外部环境和基础，数据库系统要发挥其强大的作用离不开网络系统的支持，数据库系统的用户(如异地用户、分布式用户)也要通过网络才能访问数据库的数据。网络系统的安全是数据库安全的第一道屏障，外部入侵首先就是从入侵网络系统开始的。网络入侵试图破坏信息系统的完整性、保密性或可信任的任何网络活动的集合。

网络系统开放式环境面临的威胁主要有欺骗(Masquerade)、重发(Replay)、报文修改、拒绝服务(DoS)、陷阱门(Trapdoor)、特洛伊木马(Trojanhorse)、应用软件攻击等。这些安全威胁是无时无处不在的，因此必须采取有效的措施来保障系统的安全。

2. 操作系统层次安全

操作系统是大型数据库系统的运行平台，为数据库系统提供了一定程度的安全保护。目前操作系统平台大多为 Windows NT 和 UNIX，安全级别通常为 C2 级。主要安全技术有访问控制安全策略、系统漏洞分析与防范、操作系统安全管理等。

访问控制安全策略用于配置本地计算机的安全设置，包括密码策略、账户策略、审核策略、IP 安全策略、用户权限分配、资源属性设置等，具体可以体现在用户账户、口令、访问权限和审计等方面。

3. 数据库管理系统层次安全

数据库系统的安全性在很大程度上依赖于 DBMS。如果 DBMS 的安全性机制非常完善，则数据库系统的安全性能就好。目前市场上流行的是关系型数据库管理系统，其安全性功能较弱，这就对数据库系统的安全性存在一定的威胁。

由于数据库系统在操作系统下都是以文件形式进行管理，因此入侵者可以直接利用操作系统漏洞窃取数据库文件，或者直接利用操作系统工具非法伪造、篡改数据库文件内容。

数据库管理系统层次安全技术主要是用来解决这些问题，即当前面两个层次已经被突破的情况下仍能保障数据库数据的安全，这就要求数据库管理系统必须有一套强有力的安全机制。采取对数据库文件进行加密处理是解决该层次安全的有效方法。因此，即使数据不慎泄露或者丢失，也难以被人破译和阅读。



4.3.2　数据库的审计

对于数据库系统，数据的使用、记录和审计是同时进行的。审计的主要任务是对应用程序或用户使用数据库资源的情况进行记录和审查，一旦出现问题，审计人员对审计事件记录进行分析，查出原因。因此，数据库审计可作为保证数据库安全的一种补救措施。

安全系统的审计过程是记录、检查和回顾与系统安全相关行为的过程。通过对审计记录的分析，可以明确责任个体，追查违反安全策略的违规行为。审计过程不可省略，审计记录也不可更改或删除。

由于审计行为将影响 DBMS 的存取速度和反馈时间，因此，必须综合考虑安全性系统性能，按需要提供配置审计事件的机制，以允许数据库管理员根据具体系统的安全性和性能需求做出选择。这些可由多种方法实现，如扩充、打开/关闭审计的 SQL 语句，或使用审计掩码。

数据库审计有用户审计和系统审计两种方式。

(1) 用户审计。进行用户审计时，DBMS 的审计系统记录下所有对表和视图进行访问的企图，以及每次操作的用户名、时间、操作代码等信息。这些信息一般都被记录在数据字典中，利用这些信息可以进行审计分析。

(2) 系统审计。系统审计由系统管理员进行，其审计内容主要是系统一级命令及数据库客体的使用情况。

数据库系统的审计工作主要包括设备安全审计、操作审计、应用审计和攻击审计等方面。设备安全审计主要审查系统资源的安全策略、安全保护措施和故障恢复计划等；操作审计是对系统的各种操作进行记录和分析；应用审计是审计建立于数据库上整个应用系统的功能、控制逻辑和数据流是否正确；攻击审计是指对已发生的攻击性操作和危害系统安全的事件进行检查和审计。

常用的审计技术有静态分析系统技术、运行验证技术和运行结果验证技术等。

为了真正达到审计目的，必须对记录了数据库系统中所发生过的事件的审计数据提供查询和分析手段。具体而言，审计分析要解决特权用户的身份鉴别、审计数据的查询、审计数据的格式、审计分析工具的开发等问题。

4.3.3　数据库的加密保护

大型 DBMS 的运行平台(如 Windows NT 和 UNIX)一般都具有用户注册、用户识别、任意存取控制(DAC)、审计等安全功能。虽然 DBMS 在操作系统的基础上增加了不少安全措施(如基于权限的访问控制等)，但操作系统和 DBMS 对数据库文件本身仍然缺乏有效的安全保护措施。有经验的网上黑客也会绕过一些防范屏障，直接利用操作系统工具窃取或篡改数据库文件内容，这种隐患被称为通向 DBMS 的“隐秘通道”，它所带来的危害一般数据库用户难以觉察。

在传统的数据库系统中，数据库管理员的权力至高无上，既负责各项系统的管理工作(如资源分配、用户授权、系统审计等)，又可以查询数据库中的一切信息。为此，不少系统通过各种方式来削弱系统管理员的权力。

对数据库中存储的数据进行加密是一种保护数据库数据安全的有效方法。数据库的数



据加密一般是在通用的数据库管理系统之上，增加一些加密/解密控件，来完成对数据本身的控制。与一般通信中加密的情况不同，数据库的数据加密通常不是对数据文件加密，而是对记录的字段加密。当然，在数据备份到离线的介质上送到异地保存时，也有必要对整个数据文件进行加密。

实现数据库加密以后，各用户(或用户组)的数据由用户使用自己的密钥加密，数据库管理员对获得的信息无法随意进行解密，从而保证了用户信息的安全。另外，通过加密，数据库的备份内容成为密文，从而能减少因备份介质失窃或丢失而造成的损失。由此可见，数据库加密对于企业内部安全管理也是不可或缺的。

也许有人认为，对数据库加密后会严重影响数据库系统的效率，使系统不堪重负。事实并非如此。如果在数据库客户端进行数据加/解密运算，对数据库服务器的负载及系统运行几乎没有影响。比如，在普通 PC 上，用纯软件实现 DES 加密算法的速度超过 200KB/s，如果对一篇 1 万个汉字的文章进行加密，其加密/解密时间仅需 1/10s，这种时间延迟用户几乎无感觉。目前，加密卡的加密/解密速度一般为 1Mb/s，对中小型数据库系统来说，这个速度即使在服务器端进行数据的加密/解密运算也是可行的，因为一般的关系型数据项都不会太长。

1. 数据库加密的要求

一个良好的数据库加密系统应该满足以下一些基本要求。

1) 字段加密

在目前条件下，加密/解密的粒度是每个记录的字段数据。如果以文件或列为单位进行加密，必然会形成密钥的反复使用，从而降低加密系统的可靠性，或者因加密/解密时间过长而无法使用。只有以记录的字段数据为单位进行加密/解密，才能适应数据库操作的需要，同时进行有效的密钥管理并完成“一次一密钥”的密码操作。

2) 密钥动态管理

数据库客体之间隐含着复杂的逻辑关系，一个逻辑结构可能对应着多个数据库物理客体，所以数据库加密不仅密钥量大，而且组织和存储工作较复杂，需要对密钥实行动态管理。

3) 合理处理数据

合理处理数据包括几方面的内容，首先要恰当地处理数据类型，否则 DBMS 将会因加密后的数据不符合定义的数据类型而拒绝加载；其次，需要处理数据的存储问题，实现数据库加密后，应基本上不增加空间开销。在目前条件下，数据库关系运算中的匹配字段(如表间连接码、索引字段等)数据不宜加密。

4) 不影响合法用户的操作

要求加密系统对数据操作响应的时间尽量短。在现阶段，平均延迟时间不应超过 1/10s。此外，对数据库的合法用户来说，数据的录入、修改和检索操作应该是透明的，不需要考虑数据的加密/解密问题。

2. 数据库加密的层次

可以考虑在 3 个不同层次实现对数据库数据的加密，这 3 个层次分别是操作系统层、DBMS 内核层和 DBMS 外层。

在操作系统层，无法辨认数据库文件中的数据关系，从而无法产生合理的密钥，也无法进行合理的密钥管理和使用。所以，在操作系统层对数据库文件进行加密，对于大型数据库来说，目前还难以实现。

在 DBMS 内核层实现加密，是指数据在物理存取之前完成加密/解密工作。这种方式势必造成 DBMS 和加密器(硬件或软件)之间的接口需要 DBMS 开发商的支持。这种加密方式的优点是加密功能强，并且加密功能几乎不会影响 DBMS 的功能，可以实现加密功能与数据库管理系统之间的无缝耦合。但这种方式的缺点是在服务器端进行加密/解密运算，加重了数据库服务器的负载。这种加密方式如图 4.1 所示。

比较实际的做法是将数据库加密系统做成 DBMS 的一个外层工具，如图 4.2 所示。采用这种加密方式时，加密/解密运算可以放在客户端进行，其优点是不会加重数据库服务器的负载，并可实现网上传输加密；缺点是加密功能会受到一些限制，与数据库管理系统之间的耦合性稍差。图 4.2 中“加密定义工具”模块的主要功能是定义如何对每个数据库表数据进行加密。在创建了一个数据库表后，通过这一工具对该表进行定义；“数据库应用系统”模块的功能是完成数据库定义和操作。数据库加密系统将根据加密要求自动完成对数据库数据的加密/解密操作。

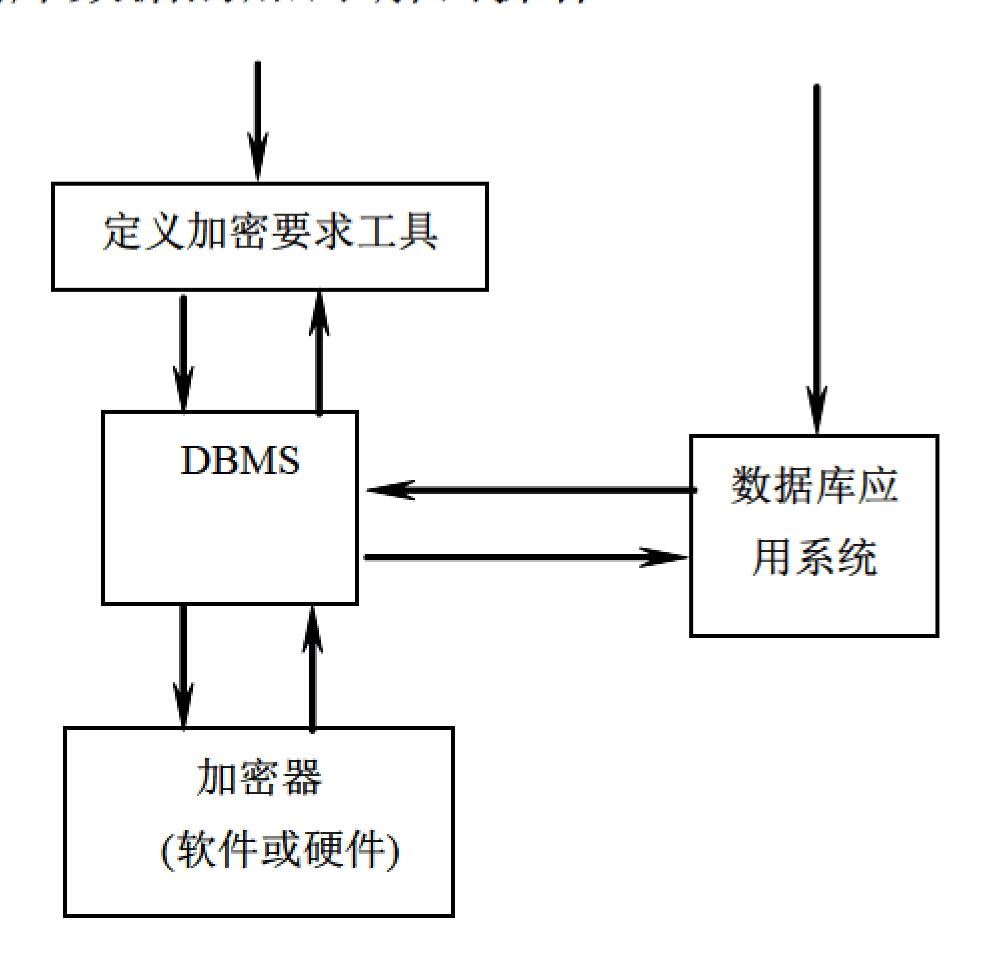


图 4.1　DBMS 内核层加密过程

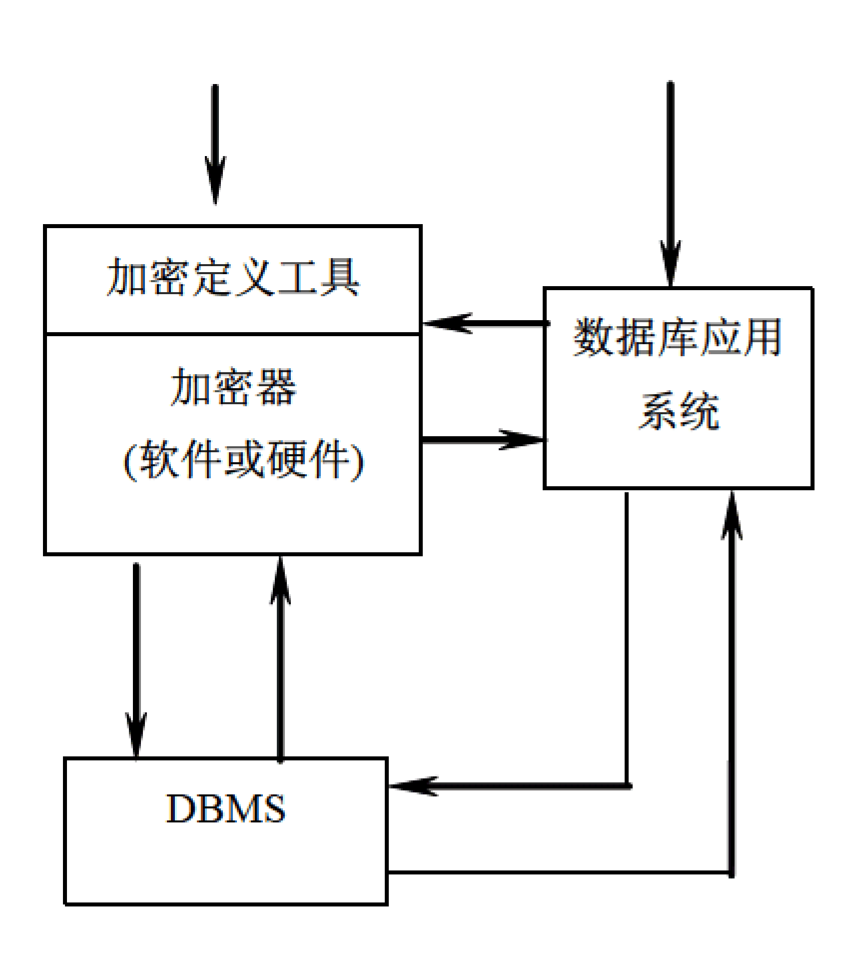


图 4.2　DBMS 外层加密过程

3. 数据库加密的有关问题

数据库加密系统首先要解决系统本身的安全性和可靠性问题，在这方面可以采用以下几项安全措施。

(1)　在用户进入系统时进行两级安全控制。

这种控制可以采用多种方式，包括设置数据库用户名和口令，或者利用工 C 卡读写器、指纹识别器进行用户身份认证。

(2)　防止非法复制。

对于纯软件系统，可以采用软指纹技术防止非法复制。当然，如果每台客户机上都安装加密卡等硬部件，安全性会更好。此外，还应该保留数据库原有的安全措施，如权限控制、备份/恢复和审计控制等。

(3)　安全的数据抽取方式。



数据库加密系统提供两种数据库中卸出和装入加密数据的方式。

① 密文方式卸出。这种卸出方式不解密，卸出的数据还是密文，在这种模式下，可直接使用 DBMS 提供的卸出/装入工具。

② 明文方式卸出。这种卸出方式需要解密，卸出的数据是明文，在这种模式下，可利用系统专用工具先进行数据转换，再使用 DBMS 提供的卸出/装入工具完成。

4. 数据库加密系统结构

数据库加密系统分成两个功能独立的主要部件：一个是加密字典管理程序；另一个是数据库加密/解密引擎。数据库加密系统体系结构如图 4.3 所示。

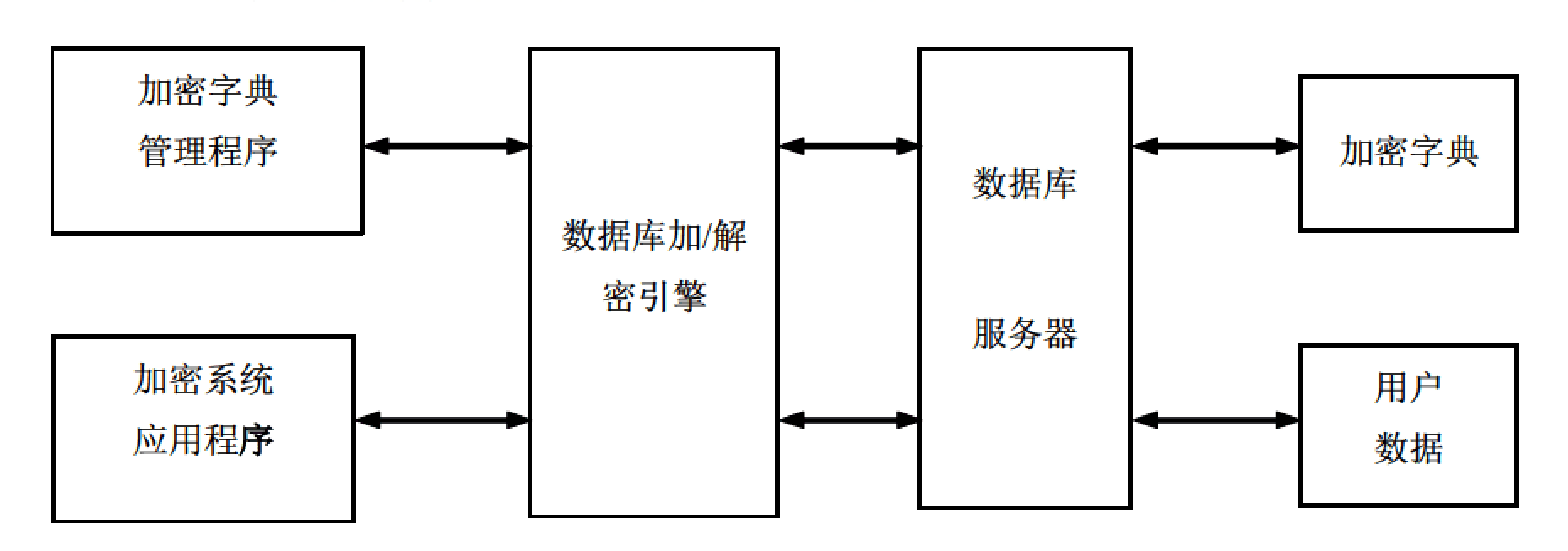


图 4.3 数据库加密系统体系结构

数据库加密系统将用户对数据库信息具体的加密要求记载在加密字典中，加密字典是数据库加密系统的基础信息，可以通过调用数据库加密/解密引擎实现对数据库表的加密、解密及数据转换等功能。数据库信息的加密/解密处理是在后台完成的，对数据库服务器是透明的。

加密字典管理程序是管理加密字典的实用程序，是数据库管理员变更加密要求的工具。加密字典管理程序通过数据库加密/解密引擎实现对数据库表的加密/解密及数据转换等功能，此时，它作为一个特殊客户来使用数据库加密/解密引擎。

数据库加密/解密引擎是数据库加密系统的核心部件，它位于应用程序与数据库服务器之间，负责在后台完成数据库信息的加密/解密处理，对应用开发人员和操作人员来说是透明的。数据加密/解密引擎没有操作界面，在需要时由操作系统自动加载并驻留在内存中，通过内部接口与加密字典管理程序和用户应用程序通信。

数据库加密/解密引擎由 3 大模块组成：数据库接口模块、用户接口模块和加密/解密处理模块。其中，数据库接口模块的主要工作是接受用户的操作请求，并传递给加密/解密处理模块；此外还要代替加密/解密处理模块去访问数据库服务器，并完成外部接口参数与加密/解密引擎内部数据结构之间的转换。加密/解密处理模块完成数据库加密/解密引擎的初始化、内部专用命令的处理、加密字典信息的检索、加密字典缓冲区的管理、SQL 命令的加密变换、查询结果的解密处理以及加密/解密算法的实现等功能，另外还包括一些公用的辅助函数。

按以上方式实现的数据库加密系统具有很多优点。

(1) 系统对数据库的最终用户完全透明，数据库管理员可以指定需要加密的数据并根据需要进行明文和密文的转换。

(2) 系统完全独立于数据库应用系统，不需要改动数据库应用系统就能实现加密功能，同时系统采用了分组加密法和二级密钥管理，实现了“一次一密钥”加密操作。

(3) 系统在客户端进行数据加密/解密运算，不会影响数据库服务器的系统效率，数据加密/解密运算基本无延迟感觉。

数据库加密系统能够有效地保证数据的安全，即使黑客窃取了关键数据，仍然难以得到所需的信息，因为所有的数据都经过了加密。另外，数据库加密以后，可以设定不需要了解数据内容的系统管理员不能见到明文，这样可大大提高关键性数据的安全性。

4.4　数据的完整性

在当今信息时代，几乎所有企事业单位的核心业务处理都依赖于计算机网络系统。在计算机网络系统中最为宝贵的就是数据。数据在计算机网络中具有两种状态：存储状态和传输状态。当数据在计算机系统数据库中保存时，处于存储状态；而在与其他用户或系统交换时，数据处于传输状态。

4.4.1　影响数据完整性的因素

数据完整性的目的就是保证网络数据库系统数据处于一种完整或未被损坏的状态。数据完整性意味着数据不会由于有意或无意的事件而被改变或丢失。相反，数据完整性的丧失，就意味着发生了导致数据被篡改或丢失的事件。为此，应首先检查造成数据完整性被破坏的原因，以便采取适当的方法予以解决，从而提高数据完整性的程度。通常，影响数据完整性的主要因素有硬件故障、软件故障、网络故障、人为威胁和意外灾难等。另外，系统数据库中的数据和存储在硬盘、光盘、软盘中的数据由于各种因素影响而失效(失去原数据功能)，这也是影响数据完整性的一个方面。

1. 硬件故障

常见的影响数据完整性的主要硬件故障有硬盘故障、I/O 控制器故障、电源故障和存储器故障等。

(1) 计算机系统运行过程中最常见的问题是硬盘故障。硬盘是一种很重要的设备，用户的文件系统、数据和软件等都存放在硬盘上。虽然每个硬盘都有一个平均无故障时间，但这并不意味着硬盘不会出问题。每次硬盘出现问题时，用户最着急的并非硬盘本身的价值，而是硬盘上存放的数据。

(2) I/O 控制器也可引起用户的数据丢失。因为 I/O 控制器有可能在某次读写过程中将硬盘上的数据删除或覆盖。这样的事情其实比硬盘故障更严重，因为硬盘出现故障时还有可能通过修复措施挽救硬盘上的数据，但如果数据完全被删除了，就无法恢复了。虽然 I/O 控制器故障发生概率很小，但它毕竟存在。

(3) 电源故障也是数据丢失的一个原因。由于电源故障可能来自外部电源停电或内部供电问题等原因，所以系统断电是不可预知的。系统突然断电时，某些存储器中的数据将会丢失。

(4) 硬盘、光盘、软盘等外存储器经常由于磕碰、振动或其他因素影响，使得存储介



质表面损坏或出现其他故障，而使数据丢失或无法读出，这些数据就失去了完整性或可用性。

此外，设备和其他备份的故障、芯片和主板故障也会引起数据的丢失。

2. 软件故障

软件故障也是威胁数据完整性的一个重要因素。常见的软件故障有软件错误、文件损坏、数据交换错误、容量错误和操作系统错误等。

软件具有安全漏洞是一个常见的问题。有的软件出错时，会对用户数据造成损坏，最可怕的事情是以超级用户权限运行的程序发生错误时，它可以把整个硬盘从根区开始删除。在应用程序之间交换数据是常有的事。当文件转换过程生成的新文件不具有正确的格式时，数据的完整性将受到威胁。

软件运行不正常的另一个原因在于资源容量达到极限。如果磁盘根区被占满，将使操作系统运行不正常，引起应用程序出错，从而导致数据丢失。

操作系统普遍存在漏洞，这是众所周知的。此外，系统的应用程序接口(API)被开发商用来为最终用户提供服务，如果这些 API 工作不正常，就会破坏数据。

3. 网络故障

网络故障通常由网卡和驱动程序问题、网络连接问题等引起。

网卡和驱动程序实际上是不可分割的，多数情况下，网卡和驱动程序故障并不损坏数据，只造成使用者无法访问数据。但当网络服务器网卡发生故障时，服务器通常会停止运行，这就很难保证被打开的那些数据文件是否被损坏。

网络中数据传输过程中，往往会由于互连设备(如路由器、网桥)的缓冲容量不够大而引起数据传输阻塞现象，从而导致数据包丢失。相反，这些互连设备也可能有较大的缓冲区，但由于调动这么大的信息流量造成的时延有可能会导致会话超时。此外，不正确的网络布线也会影响数据的完整性。

4. 人为威胁

人为活动对数据完整性造成的影响是多方面的。人为威胁使数据丢失或改变是由于操作数据的用户本身造成的。分布式系统中最薄弱的环节就是操作人员。人类易犯错误的天性是许多难以解释的错误发生的原因，比如意外事故、缺乏经验、工作压力、蓄意报复破坏和窃取等。

5. 灾难性事件

通常所说的灾难性事件有火灾、水灾、风暴、工业事故、蓄意破坏和恐怖袭击等。

灾难性事件对数据完整性有相当大的威胁。例如，美国的“9·11”事件，很多大公司和机构的数据完全被毁坏。如果没有做好备份，所造成的损失是巨大的。

灾难性事件对数据完整性之所以能造成严重的威胁，原因是灾难本身难以预料，特别是那些工业事件和恐怖袭击。另外，灾难所破坏的是包含数据在内的物理载体本身，所以，灾难基本上会将所有的数据全部毁灭。

4.4.2　保证数据完整性的方法

1. 数据完整性措施

最常用的保证数据完整性的措施是容错技术。常用的恢复数据完整性和防止数据丢失的容错技术有备份和镜像、归档和分级存储管理、转储、奇偶检验和突发事件的恢复计划等。

容错的基本思想是在正常系统基础上，利用外加资源(软、硬件冗余)来达到降低故障的影响或消除故障的目的，从而可自动地恢复系统或达到安全停机的目的。也就是说，容错是以牺牲、软硬件成本为代价达到保证系统的可靠性，如双机热备份系统。

目前容错技术将向以下方向发展：应用芯片技术容错；软件可靠性技术；高性能、高可靠性的分布式容错系统；综合性容错方法的研究等。

2. 容错系统的实现方法

常用的实现容错系统的方法有空闲备件、负载平衡、镜像、冗余系统配件和冗余存储系统等。

1)　空闲备件

空闲备件是指在系统中配置一个处于空闲状态的备用部件，它是提供容错的一条途径。当原部件出现故障时，该部件就取代原部件的功能。该容错类型的一个简单例子是将一个旧的低速打印机连在系统上，但只在当前使用的打印机出现故障时再使用该打印机，即该打印机就是系统打印机的一个空闲备件。

空闲备件在原部件发生故障时起作用，但与原部件不一定相同。

2)　负载平衡

负载平衡提供容错的途径是使两个部件共同承担一项任务，一旦其中一个部件出现故障，另一个部件就将两者的负载全部承担下来。这种方法通常在使用双电源的服务器系统中采用，如一个电源出现故障，另一个电源就承担原来两倍的负载。网络系统中常见的负载平衡是对称多处理。在对称多处理中，系统中的每一个处理器都能执行系统中的任何工作，即这种系统努力在不同的处理器之间保持负载平衡。由于该原因，对称多处理具有在 CPU 级别上提供容错的能力。

3)　镜像

镜像技术是一种在系统容错中常用的方法。在镜像技术中，两个等同的系统完成相同的任务。如果其中一个系统出现故障，另一个系统则继续工作。这种方法通常用于磁盘子系统中，两个磁盘控制器可在同样型号磁盘的相同扇区内写入相同的内容。 NetWare 系统的 SFT Ⅲ是一个典型的镜像技术，镜像要求两个系统完全相同，且完成同一个任务。

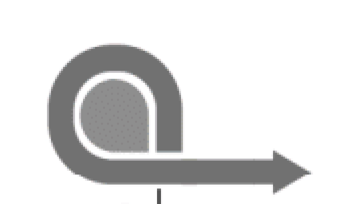
4)　冗余系统配件

冗余系统配件是指在系统中增加一些冗余配件，以增强系统故障的容错性。通常增加的冗余系统配件有电源、I/O 设备和通道、主处理器等。

5)　冗余存储系统

最常用的冗余存储系统有磁盘镜像和磁盘冗余阵列(RAID)。

(1)　磁盘镜像。



① 磁盘镜像。磁盘镜像支持在主机的一个硬盘通道上连接两块硬盘，一个为原盘，另一个为镜像盘。当主机写原盘时，同时也写了镜像盘，并对两个盘表面进行写后读验证。如果工作中原盘出现故障，镜像盘则自动承担原盘工作，数据不会丢失，系统也不会中止工作。

② 磁盘双工。磁盘镜像是用一个通道连接两个硬盘，而磁盘双工是由两个通道带两个硬盘。这样，当一个硬盘驱动器或通道控制器出现故障时，能使用另一个通道上的硬盘而不影响系统的运行。同时，系统发出警告，促使磁盘双工保护措施尽快地得到恢复。

(2) 独立磁盘冗余阵列 RAID。

RAID(Redundant Array of Independent Disks，独立磁盘冗余阵列，简称磁盘阵列)可采用硬件或软件的方法实现。磁盘阵列由磁盘控制器和多个磁盘驱动器组成，由磁盘控制器控制和协调多个磁盘驱动器的读、写操作。根据使用的 RAID 级别，一个数据文件可以采取不同的方式写入多个磁盘，从而提高性能。RAID 是一种能够在不经历任何故障时间的情况下更换正在出错的磁盘或已发生故障的磁盘的存储系统，它是保证磁盘子系统非故障时间的一条途径。RAID 的初衷主要是为大型服务器提供高端的存储功能和冗余的数据安全。可以这样来理解，RAID 是一种把多块独立的硬盘(物理硬盘)按不同方式组合起来形成一个硬盘组(逻辑硬盘)，从而提供比单个硬盘更高的存储性能和提供数据冗余的技术。组成磁盘阵列的不同方式便成为 RAID 级别划分的标准。在用户看起来，组成的磁盘组就像是一个硬盘。用户可以对它进行分区、格式化等。不同的是，磁盘阵列的存储性能要比单个硬盘高很多，而且在很多 RAID 模式中都有较为完备的相互校检/恢复措施，甚至是直接相互的镜像备份，从而大大提高了 RAID 系统的容错度，提高了系统的稳定冗余性。

不过，所有的 RAID 系统最大的优点则是“热交换”能力：用户可以取出一个存在缺陷的驱动器，并插入一个新的驱动器予以更换。对大多数类型的 RAID 来说，可以利用镜像或奇偶信息在其他冗余的驱动器中重建数据，而不必中断服务器或系统，就可以自动重建某个出现故障的磁盘上的数据。这一点对服务器用户以及其他高要求的用户是至关重要的。

数据冗余的功能是指用户数据一旦发生损坏后，利用冗余信息可以使损坏数据得以恢复，从而保障了用户数据的完整性。

RAID 技术经过不断的发展，现在已拥有从 RAID 0 到 RAID 6 等 7 种基本的级别。另外，还有一些基本 RAID 级别的组合形式，如 RAID 10(RAID 0 与 RAID 1 的组合)、RAID 50(RAID 0 与 RAID 5 的组合)等。不同 RAID 级别代表着不同的存储性能、数据安全性和存储成本。

4.5 数据备份和恢复

在日常工作中，人为操作错误、系统软件或应用软件缺陷、硬件损毁、计算机病毒、黑客攻击、突然断电、意外宕机、自然灾害等诸多因素都有可能造成计算机中数据的丢失，给企业造成无法估量的损失。数据的丢失极有可能演变成一场灭顶之灾。因此，数据备份与恢复对企业来说显得格外重要。



4.5.1　数据备份

1. 数据备份的概念

数据备份就是指为防止系统出现操作失误或系统故障导致数据丢失，而将全系统或部分数据集合从应用主机的硬盘或阵列中复制到其他存储介质上的过程。计算机系统中的数据备份，通常是指将存储在计算机系统中的数据复制到磁带、磁盘、光盘等存储介质上，在计算机以外的地方另行保管。这样，当计算机系统设备发生故障或发生其他威胁数据安全的灾害时，能及时地从备份的介质上恢复正确的数据。

数据备份的目的就是为了系统数据崩溃时能够快速地恢复数据，使系统迅速恢复运行。那么就必须保证备份数据和源数据的一致性和完整性，消除系统使用者的后顾之忧。其关键在于保障系统的高可用性，即操作失误或系统故障发生后，能够保障系统的正常运行。

如果没有了数据，一切的恢复都是不可能实现的，因此备份是一切灾难恢复的基石。从这个意义上说，任何灾难恢复系统实际上都是建立在备份基础上的。

现在不少企业也意识到了这一点，采取了系统定期检测与维护、双机热备份、磁盘镜像或容错、备份磁带异地存放、关键部件冗余等多种预防措施。这些措施一般能够进行数据备份，并且在系统发生故障后能够快速进行系统恢复。

数据备份和恢复系统通过将计算机系统中的数据进行备份和脱机保存后，当系统中的数据因任何原因丢失、混乱或出错时，即可将原备份的数据从备份介质中恢复回系统，使系统重新工作。数据备份与恢复系统是数据保护措施中最直接、最有效、最经济的方案，也是任何计算机信息系统不可缺少的一部分。

数据备份能够用一种增加数据存储代价的方法保护数据安全，它对于拥有重要数据的大企事业单位是非常重要的，因此数据备份和恢复通常是大中型企事业单位的网络系统管理员每天必做的工作之一；对于个人计算机用户，数据备份也是非常必要的。

传统的数据备份主要是采用数据内置或外置的磁带机进行冷备份。一般来说，各种操作系统都附带了备份程序。但是随着数据的不断增加和系统要求的不断提高，附带的备份程序根本无法满足需求。要想对数据进行可靠的备份，必须选择专门的备份软、硬件，并制订相应的备份及恢复方案。

目前比较常用的数据备份有以下几种。

(1)　本地磁带备份。利用大容量磁带备份数据。

(2)　本地可移动存储器备份。利用大容量等价软盘驱动器、可移动等价硬盘驱动器、一次性可刻录光盘驱动器、可重复刻录光盘驱动器进行数据备份。

(3)　本地可移动硬盘备份。利用可移动硬盘备份大量的数据。

(4)　本机多硬盘备份。在本机内装有多块硬盘，利用除安装和运行操作系统和应用程序的一块或多块硬盘外的其余硬盘进行数据备份。

①　远程磁带库、光盘库备份。将数据传送到远程备份中心制作完整的备份磁带或光盘。

②　远程关键数据加磁带备份。采用磁带备份数据，生产机实时向备份机发送关键数据。

③　远程数据库备份。在与主数据库所在生产机相分离的备份机上建立主数据库的一



个备份。

④ 网络数据镜像。对生产系统的数据库数据和所需跟踪的重要目标文件的更新进行监控与跟踪，并将更新日志实时通过网络传送到备份系统，备份系统则根据日志对磁盘进行更新。

⑤ 远程镜像磁盘。通过高速光纤通道线路和磁盘控制技术将镜像磁盘延伸到远离生产机的地方，镜像磁盘数据与主磁盘数据完全一致，更新方式为同步或异步。

2. 数据备份的类型

按数据备份时数据库状态的不同可分为冷备份、热备份和逻辑备份等类型。

1) 冷备份(Coldbackup)

冷备份是指在关闭数据库的状态下进行的数据库完全备份。备份内容包括所有的数据文件、控制文件、联机日志文件、ini 文件等。因此，在进行冷备份时数据库将不能被访问。冷备份通常只采用完全备份。

2) 热备份(Hotbackup)

热备份是指在数据库处于运行状态下，对数据文件和控制文件进行的备份。使用热备份必须将数据库运行在归档(Archivelog)方式下，因此，在进行热备份的同时可以进行正常数据库的各种操作。

3) 逻辑备份

逻辑备份是最简单的备份方法，可按数据库中某个表、某个用户或整个数据库进行导出。使用这种方法，数据库必须处于打开状态，而且如果数据库不是在 Restrict 状态将不能保证导出数据的一致性。

3. 数据备份策略

需要进行数据备份的部门都要先制定数据备份策略。数据备份策略包括确定需备份的数据内容(如进行完全备份、增量备份、差别备份还是按需备份)、备份类型(如采用冷备份还是热备份)、备份周期(如以月、周、日还是小时为备份周期)、备份方式(如采用手工备份还是自动备份)、备份介质(如以光盘、硬盘、磁带还是 U 盘做备份介质)和备份介质的存放等。下面是不同数据内容的几种备份方式。

1) 完全备份(Full Backup)

完全备份是指按备份周期(如一天)对整个系统所有文件(数据)进行备份。这种备份方式比较流行，也是克服系统数据不安全的最简单方法，操作起来也很方便。有了完全备份，网络管理员可清楚地知道从备份之日起便可恢复网络系统的所有信息，恢复操作也可一次性完成。如发现数据丢失时，只要用一盘故障发生前一天备份的磁带，即可恢复丢失的数据。但这种方式的不足之处是由于每天都对系统进行完全备份，在备份数据中必定有大量的内容是重复的，这些重复的数据占用了大量的磁带空间，这对用户来说就意味着增加成本。另外，由于进行完全备份时需要备份的数据量相当大，因此备份所需时间较长。对于那些业务繁忙，备份窗口时间有限的单位来说，选择这种备份策略是不合适的。

2) 增量备份(Incremental Backup)

增量备份是指每次备份的数据只是相当于上一次备份后增加的和修改过的内容，即备份的都是已更新过的数据。比如，系统在星期日做了一次完全备份，然后在以后的 6 天里

每天只对当天新的或被修改过的数据进行备份。这种备份的优点很明显，没有或减少了重复的备份数据，既节省存储介质空间，又缩短了备份时间。但它的缺点是恢复数据过程比较麻烦，不可能一次性地完成整体的恢复。

3)　差别备份(Different Backup)

差别备份也是在完全备份后将新增加或修改过的数据进行备份，但它与增量备份的区别是每次备份都把上次完全备份后更新过的数据进行备份。比如，星期日进行完全备份后，其余 6 天中的每一天都将当天所有与星期日完全备份时不同的数据进行备份。差别备份可节省备份时间和存储介质空间；只需两盘磁带(星期日备份磁带和故障发生前一天的备份磁带)即可恢复数据。差别备份兼具了完全备份发生数据丢失时恢复数据较方便和增量备份节省存储介质空间及备份时间的优点。

完全备份所需的时间最长，占用存储介质容量最大，但数据恢复时间最短、操作最方便，当系统数据量不大时该备份方式最可靠；但当数据量增大时，很难每天都做完全备份，可选择周末做完全备份，在其他时间采用所用时间最少的增量备份或时间介于两者之间的差别备份。在实际备份应用中，通常也是根据具体情况，采用这几种备份方式的组合，如年底做完全备份，月底做完全备份，周末做完全备份，而每天做增量备份或差别备份。

4)　按需备份

除以上备份方式外，还可采用对随时所需数据进行备份的方式进行数据备份。按需备份，就是指除正常备份外，额外进行的备份操作。额外备份可以有许多理由，比如，只想备份很少几个文件或目录、备份服务器上所有必需的信息以便进行更安全的升级等。这样的备份在实际中经常遇到，它可弥补冗余管理或长期转储的日常备份的不足。

4.5.2　数据恢复

数据恢复是指将备份到存储介质上的数据再恢复到计算机系统中，它与数据备份是一个相反的过程。

数据恢复措施在整个数据安全保护中占有相当重要的地位，因为它关系到系统在经历灾难后能否迅速恢复运行。

通常，在遇到下列情况时应使用数据恢复功能进行数据恢复。

(1)　当硬盘数据被破坏时。

(2)　当需要查询以往年份的历史数据，而这些数据已从现系统上清除。

(3)　当系统需要从一台计算机转移到另一台计算机上运行时，可将使用的相关数据恢复到新计算机的硬盘上。

1. 恢复数据时的注意事项

(1)　由于恢复数据是覆盖性的，不正确的恢复可能破坏硬盘中的最新数据，因此在进行数据恢复时，应先将硬盘数据备份。

(2)　进行恢复操作时，用户应指明恢复何年何月的数据。当开始恢复数据时，系统首先识别备份介质上标识的备份日期是否与用户选择的日期相同，如果不同将提醒用户更换备份介质。

(3)　由于数据恢复工作比较重要，容易错把系统上的最新数据变成备份盘上的旧数据，



因此应指定少数人进行此项操作。

(4) 不要在恢复过程中关机、关电源或重新启动机器。

(5) 不要在恢复过程中打开驱动器开关或抽出软盘、光盘，除非系统提示换盘。

2. 数据恢复的类型

一般来说，数据恢复操作比数据备份操作更容易出问题。数据备份只是将信息从磁盘复制出来，而数据恢复则要在目标系统上创建文件。在创建文件时会出现许多差错，如超过容量限制、权限问题和文件覆盖错误等。数据备份操作无须知道太多的系统信息，只需复制指定信息即可；而数据恢复操作则需要知道哪些文件需要恢复，哪些文件不需要恢复等。

数据恢复操作通常可分为 3 类：全盘恢复、个别文件恢复和重定向恢复。

1) 全盘恢复

全盘恢复就是将备份到介质上的指定系统信息全部转储到它们原来的地方。全盘恢复一般应用在服务器发生意外灾难时导致数据全部丢失、系统崩溃或是有计划的系统升级、系统重组等，也称为系统恢复。

2) 个别文件恢复

个别文件恢复就是将个别已备份的最新版文件恢复到原来的地方。对大多数备份来说，这是一种相对简单的操作。个别文件恢复要比全盘恢复常用得多。利用网络备份系统的恢复功能，很容易恢复受损的个别文件(数据)。需要时只要浏览备份数据库或目录，找到该文件(数据)，启动恢复功能，系统将自动驱动存储设备，加载相应的存储媒体，恢复指定文件(数据)。

3) 重定向恢复

重定向恢复是将备份的文件(数据)恢复到另一个不同的位置或系统上去，而不是做备份操作时它们所在的位置。重定向恢复可以是整个系统恢复，也可以是个别文件恢复。进行重定向恢复时需要慎重考虑，要确保系统或文件恢复后的可用性。

4.6 网络备份系统

4.6.1 单机备份和网络备份

数据备份对使用计算机的人来说并不陌生，每个人都可能曾经做过一些重要文件的备份。早期的数据备份通常是采用单个主机内置或外置的磁带机或磁盘机对数据进行冷备份。这种单机式备份在数据量不大、操作系统简单、服务器数量少的情况下，是一种既经济又简单、实用的备份手段。但随着网络技术的发展和广泛应用，以及数据量爆炸性的增长，单机备份方式越来越不适应网络系统环境，产生了诸多不利，比如：

(1) 数据分散在不同机器、不同应用上，管理分散，安全得不到保障。

(2) 难以实现数据库数据的高效热备份。

(3) 备份时不能缺少维护人员，工作效率低。

(4) 存储介质管理难度大。

(5) 数据丢失现象难以避免。

(6) 灾难给系统重建和业务数据运作带来困难。

网络系统备份不仅备份系统中的数据，而且还可备份系统中的应用程序、数据库系统、用户设置、系统参数等信息，以便迅速恢复整个系统。网络系统备份是全方位、多层次的备份，但并非所有情况下都要备份系统信息，因为有些应用只需将系统中的重要数据进行备份即可。数据备份主要是进行系统中重要数据(特别是数据库)的备份。

在备份过程中，如果只管理一台计算机，进行单机备份，那么备份事件就很简单。但如果管理多台计算机或一个网段，甚至整个企业网，备份就是一件非常复杂的事情。数据备份的核心是数据库备份，流行的数据库系统(如 Oracle、Sybase)均有自己的数据库备份工具，但它们不能实现自动备份，只能将数据备份到磁带机或硬盘上，而不能驱动磁带库等自动加载设备。采用具有自动加载功能的磁带库硬件产品与数据库在线备份功能的自动备份软件，即可满足用户的要求。目前流行的备份软件都具有自动定时备份管理、备份介质自动管理、数据库在线备份管理等功能。Legato 公司的 NetWorker 和 Veritas 公司的 NetBackup 系统可跨平台进行网络数据的自动备份管理，可实现备份系统的分布式处理、集中式管理、备份机器分组管理、备份介质分组管理、备份数据分类分组管理及备份介质自动重复使用等多项功能。备份的数据可在每个备份客户机上按需恢复，也可在同平台上按用户权限交叉恢复，而备份操作可采用集中自动执行或手动执行。

理想的备份系统应该是全方位的、多层次的。比如，使用网络存储备份系统和硬件容错相结合的方式，就可以恢复由于硬件故障、软件故障或人为错误造成的损坏。这种结合方式构成了对系统软、硬件的多级保护，既可以防止物理损坏，又能较好地防止逻辑损坏。

网络备份系统的功能是尽可能快地全面恢复运行计算机系统所需的数据和系统信息。网络备份系统对整个网络的数据进行管理。网络备份系统既要能在由于系统或人为故障造成系统数据损坏或丢失后，可及时地实现数据的恢复，又要能在发生地域灾难时及时地在本地或异地实现数据及整个系统的灾难恢复。

网络备份实际上不仅是指网络上各计算机的文件备份，而是包括了整个网络系统的一套备份体系。该体系包括文件备份和恢复、数据库备份和恢复，系统灾难恢复和备份任务管理等。

4.6.2　网络备份系统的组成

所有的数据可以备份到与备份服务器或应用服务器相连的一台备份介质中。一个网络备份系统由目标、工具、存储设备和通道 4 个部件组成。

(1) 目标是指被备份或恢复的系统。一个完整的自动备份系统，在目标中都要运行一个备份客户程序。该程序允许远程对目标进行相应的文件操作，这样可以实现集中式、全自动备份的功能。

(2) 工具是执行备份或恢复任务的系统。工具提供一个集中管理控制平台，管理员可以利用该平台去配置整个网络备份系统。

(3) 存储设备就是备份的数据被保存的地方，通常有磁带、磁盘等。存储设备和工具可以在一台机器中，也可以在不同的机器中。

(4) 通道是指将存储设备与网络计算机连接在一起的线路和接口等，其作用就是作为目标、工具与存储设备之间的逻辑通路，为备份数据或恢复数据提供通道。



网络备份系统可实现备份和恢复两个过程。前者就是利用工具将目标备份到存储设备中；后者是利用工具将存储设备中的数据恢复到目标中。

一个完整的网络备份系统组成可包括备份计划、备份管理及操作员、网络管理系统、主机系统、目标系统、工具系统、存储设备及其启动程序、I/O 通道和外围设备等。

实际的网络备份系统通常是由物理主机系统、逻辑主机系统、I/O 总线、外围设备、设备驱动程序、备份存储介质、备份计划文档、操作执行者、物理目标系统、逻辑目标系统、网络连接和网络协议等组成的。

4.6.3 网络备份系统方案

在谈到数据备份时，有人总认为只要将数据复制后保存起来，就可以确保数据的安全，其实，这是对备份的误解，因为资料、数据的复制根本无法完成对历史记录的追踪，也无法留下系统信息，这样做只能是在系统完好的情况下，将部分数据进行恢复。

实际上，备份不仅只是对数据的保护，其最终目的是为了在系统遇到人为或自然灾难时，能够通过备份内容对系统进行有效的恢复。所以，在考虑备份选择时，应该不仅只是消除传统输入复杂程序或手动备份的麻烦，更要能实现自动化及跨平台的备份，满足用户的全面需求。因此，备份不等于单纯的复制，管理也是备份重要的组成部分。管理包括备份的可计划性、磁带机的自动化操作、历史记录的保存及日志记录等。正是有了这些先进的管理功能，在恢复数据时才能掌握系统信息和历史记录，使备份真正实现轻松和可靠。

一个完整的网络备份和灾难恢复方案应包括备份硬件、备份软件、备份计划和灾难恢复计划 4 个部分。

1. 备份硬件

一般说来，丢失数据有 3 种可能，即人为的错误、漏洞与病毒影响、设备失灵。目前比较流行的硬件备份解决方法包括硬盘存储、光学介质和磁带/磁带机存储备份技术。

与磁带/磁带机存储技术和光学介质备份相比，硬盘存储所需费用是极其昂贵的。磁盘存储技术虽然可以提供容错性解决方案，但容错却不能抵御用户的错误和病毒。一旦两个磁盘在短时间内失灵，在一个磁盘重建之前，不论是磁盘镜像还是磁盘双工都不能提供数据保护。因此，在大容量数据备份方面，采用硬盘作为备份介质并不是最佳选择。

与硬盘备份相比，虽然光学介质备份提供了比较经济的存储解决方案，但它们所用的访问时间要比硬盘多几倍，并且容量相对较小。当备份大容量数据时，所需光盘数量多，虽保存的时间较长，但整体可靠性较低。所以光学介质也不是大容量数据备份的最佳选择。

利用磁带机进行大容量的信息备份具有容量大、可灵活配置、速度相对适中、介质保存长久(存储时间超过 30 年)、成本较低、数据安全性高、可实现无人操作的自动备份等优势。所以一般来说，磁带设备是大容量网络备份用户的主要选择。

2. 备份软件

可能大多数用户还没有意识到备份软件的重要性，其重要原因是许多人对备份知识和备份手段缺乏了解。他们所知道的备份软件无非是网络操作系统附带提供的备份功能，但对如何正确使用专业的备份软件却知之甚少。

备份软件主要分为两大类：一类是各个操作系统厂商在操作系统软件内附带的备份功能，(如 NetWare 操作系统的 Backup 功能、NT 操作系统的 NTBackup 等)；另一类是各个专业厂商提供的全面的专业备份软件，如 HP Open View Omni Back Ⅱ和 CA 公司的 ARCServerIT 等。

对于备份软件的选择，不仅要注重使用方便、自动化程度高，还要有好的扩展性和灵活性。同时，跨平台的网络数据备份软件能满足用户在数据保护、系统恢复和病毒防护等方面的支持。一个专业的备份软件配合高性能的备份设备，能够使遭损坏的系统迅速得以恢复。

3. 备份计划

灾难恢复的先决条件是要做好备份策略及恢复计划。日常备份计划描述每天的备份以什么方式进行、使用什么介质、什么时间进行以及系统备份方案的具体实施细则。在计划制订完毕后，应严格按照程序进行日常备份，否则将无法达到备份的目的。

在备份计划中，数据备份方式的选择是主要的。目前的备份方式主要有完全备份、增量备份和差别备份。用户根据自身业务对备份内容和灾难恢复的要求，应该进行不同的选择，也可以将这几种备份方式进行组合应用，以得到更好的效果。

4. 灾难恢复计划

灾难恢复计划在整个备份中占有相当重要的地位。因为它关系到系统、软件与数据在经历灾难后能否快速、准确地恢复。全盘恢复一般应用在服务器发生意外灾难，导致数据全部丢失、系统崩溃或是有计划的系统升级、系统重组等情况，也称为系统恢复。此外，有些厂商还推出了拥有单键恢复功能的磁带机，只需用系统盘引导机器启动，将磁带插入磁带机，按动一个按键即可恢复整个系统。

4.7 数 据 容 灾

对于 IT 而言，容灾系统就是为计算机信息系统提供的一个能应付各种灾难的环境。当计算机系统在遭受如火灾、水灾、地震、战争等不可抗拒的灾难和意外时，容灾系统将保证用户数据的安全性(数据容灾)。甚至，一个更加完善的容灾系统还能提供不间断的应用服务(应用容灾)。可以说，容灾系统是存储应用的最高境界。

4.7.1 数据容灾概述

1. 容灾系统和容灾备份

这里所说的“灾”具体是指计算机网络系统遇到的自然灾难(洪水、飓风、地震)、外在事件(电力或通信中断)、技术失灵及设备受损(火灾)等。容灾(或容灾备份)就是指计算机网络系统在遇到这些灾难时仍能保证系统数据的完整性、可用性和系统正常运行。

对于那些业务不能中断的用户和行业(如银行、证券、电信等)，因为其关键业务的特殊性，必须有相应的容灾系统进行防护。保持业务的连续性是当今企业用户需要考虑的一个极为重要的问题，而容灾的目的就是保证关键业务的可靠运行。利用容灾系统，用户把



关键数据存放在异地，当生产中心发生灾难时，备份中心可以很快将系统接管并运行起来。

从概念上讲，容灾备份是指通过技术和管理的途径，确保在灾难发生后，企事业单位的关键数据、数据处理系统和业务在短时间内能够恢复。因此，在实施容灾备份项目之前，企事业单位首先要分析哪些数据最重要，哪些数据要做备份、容灾，这些数据价值多少，再决定采用何种形式的容灾备份。

在欧美发达国家，企业对容灾备份的投入相对是较高的。据国外权威机构调查，2002年，全球2000家大型企业用于容灾备份的资金占企业IT支出的2%～4%，而当年关于容灾备份的支出则是2000年的3倍。在国内，越来越多的企业也已经意识到存储信息的重要性，正处于从数据分散存储向集中存储转变的过程，开始投资搭建存储系统。但还有许多企业没有意识到容灾备份是信息存储的一个重要环节。

目前国内专门提供容灾服务的备份中心还处于起步阶段，虽然有一些由电信企业提供的容灾备份中心，但由于大部分企业对容灾备份中心及提供的服务并不了解，因而利用率不高。

现在，容灾备份的技术和市场正处于一个快速发展的阶段。据权威机构研究表明，亚太地区(不包括日本)容灾备份市场每年增幅有20%，到2006年将达到13亿美元，而中国市场每年的增幅将达到46%，这是一个尚待开采的“金矿”。在此契机下，国家已将容灾备份作为今后信息发展规划中的一个重点，各地方和行业准备或已建立起一些容灾备份中心。这不仅可以为大型企业和部门提供容灾服务，也可以为大量的中小企业提供不同需求的容灾服务。

2. 数据容灾与数据备份的关系

许多用户对经常听到的数据容灾这种说法不理解，把数据容灾与数据备份等同起来，其实这是错误的，至少是不全面的。

备份与容灾不是等同的关系，而是两个“交集”，中间有大部分的重合关系。多数容灾工作可由备份来完成，但容灾还包括网络等其他部分，而且只有容灾才能保证业务的连续性。所以说，如果对容灾的要求高，仅仅依赖备份是不够的。但目前，国内很多客户、系统集成商认为，容灾就是将两套存储设备连接起来，这种观点是片面的。

数据容灾与数据备份的关系主要体现在以下几个方面。

1) 数据备份是数据容灾的基础

数据备份是数据高可用性的一道安全防线，其目的是为了在系统数据崩溃时能够快速地恢复数据。虽然它也算一种容灾方案，但这样的容灾能力非常有限，因为传统的备份主要是采用数据内置或外置的磁带机进行冷备份，备份磁带同时也在机房中统一管理，一旦整个机房出现了灾难(如火灾、盗窃和地震等)，这些备份磁带也将随之销毁，所存储的磁带备份将起不到任何容灾作用。

2) 容灾不是简单备份

显然，容灾备份不等同于一般意义上的业务数据备份与恢复。数据备份与恢复只是容灾备份中的一部分。容灾备份系统还包括最大范围的容灾、最大限度地减少数据丢失、实时切换、短时间恢复等多项内容。可以说，容灾备份正在成为保护企事业单位关键数据的一种有效手段。容灾备份系统的核心技术是数据复制。

真正的数据容灾就是要避免传统冷备份所具有的先天不足，要能在灾难发生时全面、及时地恢复整个系统。容灾按其能力的高低可分为多个层次，如国际标准 SHARE 78 定义的容灾系统有 7 个层次，从最简单的仅在本地进行磁带备份，到将备份的磁带存储在异地，再到建立应用系统实时切换的异地备份系统，恢复时间最少是几天或几小时，甚至到分钟级、秒级或零数据丢失等。

无论采用哪种容灾方案，数据备份还是最基础的，没有备份的数据，任何容灾方案都没有现实意义。但仅有备份是不够的，容灾也必不可少。容灾对于 IT 而言，就是提供一个能防止各种灾难的计算机信息系统。

3)　容灾不仅仅是技术

容灾不仅仅是一项技术，更是一项工程。目前很多客户还停留在对容灾技术的关注上，而对容灾的流程、规范及其具体措施还不太清楚，也从不对容灾方案的可行性进行评估，认为只要建立了容灾方案即可放心了，其实这是具有很大风险的。特别是在一些中小企事业单位中，认为自己的企事业单位为了数据备份和容灾，年年花费了大量的人力和财力，而结果几年下来根本就没有发生过任何大的灾难，于是放松了警惕。可一旦发生了灾难，将损失巨大。这一点国外的跨国公司就做得非常好，尽管几年下来的确未出现大的灾难，备份了那么多磁带，几乎没有派上任何用场，但仍一如既往非常认真地做好每一步，并且基本上每月都有对现行容灾方案的可行性进行评估，进行实地演练。

3. 数据容灾的等级

设计一个容灾备份系统，需要考虑多方面的因素，如备份/恢复数据量的大小、应用数据中心和备援数据中心之间的距离和数据传输方式、灾难发生时所要求的恢复速度、备援中心的管理及投入等。根据这些因素和不同的应用场合，常见的容灾备份可分为以下 4 个等级。

(1)　第 0 级：本地复制、本地保存的冷备份。

第 0 级容灾备份，实际上就是上面所指的数据备份。它的容灾恢复能力最弱，只在本地进行数据备份，并且备份的数据磁带保存在本地，没有送往异地。

在这种容灾方案中，最常用的设备就是磁带机，当然根据实际需要可以是手工加载磁带机，也可以是自动加载磁带机。如 IBM 的 TotalStorage Ultrium 外置式磁带机 3580，单盒磁盘容量可达 200GB，压缩后可存储 400GB 数据，可满足绝大多数中小企事业单位乃至大型企事业单位的数据备份需求。

(2)　第 1 级：本地复制、异地保存的冷备份。

在本地将关键数据备份，然后送到异地保存，如交由银行保管。灾难发生后，按预定数据恢复程序恢复系统和数据。这种容灾方案也是采用磁带机等存储设备进行本地备份，同样还可以选择磁带库、光盘库等进行备份。

常见到一些公司为了避免备份磁带因机房安全问题而出现磁带被盗、被毁，把备份磁带，特别是月以上的备份磁带放入专门的保险柜，甚至租用银行的专门保险箱来存放这些备份磁带。但这还不能说是万无一失，原因就是一般这些保管磁带的地点与所在公司在同一城市中，万一出现了地震、战争之类的自然灾难，这些备份磁带还是难逃厄运。

(3)　第 2 级：热备份站点备份。



第 2 级是指在异地建立一个热备份点，通过网络进行数据备份。也就是通过网络以同步或异步方式，把主站点的数据复制到备份站点。备份站点一般只备份数据，不承担其他业务。当出现灾难时，备份站点接替主站点的业务，从而维护业务系统运行的连续性。

这种异地远程数据容灾方案的容灾地点通常要选择在距离本地不小于 20km 的范围，采用与本地磁盘阵列相同的配置，通过光纤以冗余方式接入到 SAN(存储区域网)网络中实现本地关键应用数据的实时同步复制。在本地数据及整个应用系统出现灾难时，系统至少在异地保存一份可用的关键业务的备份数据。该数据是本地数据的完全实时复制。对于较大的企事业单位网络来说，建立的数据容灾系统由主数据中心和备份数据中心组成。其中，主数据中心采用高可靠性集群解决方案设计，备份数据中心与主数据中心通过光纤相连接。数据存储在主数据中心的存储磁盘阵列中，同时，在异地备份数据中心配置相同结构的存储磁盘阵列和一台或多台备份服务器。通过专用的灾难恢复软件可以自动实现主数据中心的存储数据与备份数据中心数据的实时完全备份。在主数据中心，按照用户要求，还可以配置磁带备份服务器，用来安装备份软件和磁带库。备份服务器直接连接到存储阵列和磁带库，控制系统的日常数据的磁带备份。两个数据中心利用它们之间的光传输设备，通过光纤组成光自愈环，可提供总共高达 80Gb/s(保护)和 160Gb/s(非保护)的通信带宽。

(4) 第 3 级：活动互援备份。

活动互援备份异地容灾方案与前面介绍的热备份站点备份方案差不多，其中的备份数据中心就是备援数据中心。不同的只是主、从系统的关系不再是固定的，而是互为对方的备份系统。这两个数据中心系统分别在相隔较远的地方建立，它们都处于工作状态，并进行相互数据备份。当某个数据中心发生灾难时，另一个数据中心接替其工作任务。通常在这两个系统中的光纤设备连接中还提供冗余通道，以备工作通道出现故障时及时接替工作。当然，采取这种容灾方式的主要是资金实力较为雄厚的大型企事业单位。

该级别的容灾备份根据实际要求和投入资金的多少，可有两种实现形式。

① 两个数据中心之间只限于关键数据的相互备份。

② 两个数据中心之间互为镜像。

两个数据中心之间互为镜像可做到零数据丢失，这是目前要求最高的一种容灾备份方式，它要求不管什么灾难发生，系统都能保证数据的安全。所以，它需要配置复杂的管理软件和专用的硬件设备，需要的投资相对是最大的，但恢复速度也是最快的。

以上第 2 级、第 3 级两种热备份方式不再是传统的磁带冷备份方式，而是通过 SAN 等先进的通道技术，把服务器数据同步或异步存储在远程专用存储设备上。在这两种热备份容灾方案中，主要的备份设备包括磁盘阵列、光纤交换机或磁盘机等。

4. 容灾系统

容灾系统包括数据容灾和应用容灾两部分。数据容灾可保证用户数据的完整性、可靠性和一致性，但不能保证服务不被中断。应用容灾是在数据容灾的基础上，在异地建立一套完整的与本地生产系统相当的备份应用系统，在灾难情况下，远程系统迅速接管业务运行，提供不间断的应用服务，让客户的服务请求能够继续。可以说，数据容灾是系统能够正常工作的保障；而应用容灾则是容灾系统建设的目标，它是建立在可靠的数据容灾基础上，通过应用系统、网络系统等各种资源之间的良好协调来实现的。



1)　本地容灾

本地容灾的主要手段是容错。容错的基本思想就是利用外加资源的冗余技术来达到屏蔽故障、自动恢复系统或安全停机的目的。容错是以牺牲外加资源为代价来提高系统可靠性的。外加资源的形式很多，主要有硬件冗余、时间冗余、信息冗余和软件冗余。容错技术的使用使得容灾系统能恢复大多数的故障，然而当遇到自然灾害及战争等意外时，仅采用本地容灾技术并不能满足要求，这时应考虑采用异地容灾保护措施。

在系统设计中，企业一般考虑做数据备份和采用主机集群的结构，因为它们能解决本地数据的安全性和可用性。目前人们所关注的容灾，大部分也都只是停留在本地容灾的层面上。

2)　异地容灾

异地容灾是指在相隔较远的异地，建立两套或多套功能相同的系统。当主系统因意外原因停止工作时，备用系统可以接替工作，保证系统的不间断运行。异地容灾系统采用的主要方法是数据复制，目的是在本地与异地之间确保各系统关键数据和状态参数的一致。

异地容灾系统具备应对各种灾难特别是区域性与毁灭性灾难的能力，具备较为完善的数据保护与灾难恢复功能，保证灾难降临时数据的完整性及业务的连续性，并在最短时间内恢复业务系统的正常运行，将损失降到最小。其系统一般由生产系统、可接替运行的后备系统、数据备份系统、备用通信线路等部分组成。在正常生产和数据备份状态下，生产系统向备份系统传送需备份的数据。灾难发生后，当系统处于灾难恢复状态时，备份系统将接替生产系统继续运行。此时重要营业终端用户将从生产主机切换到备份中心主机，继续对外营业。

从广义上讲，任何提高系统可用性的努力都可称为容灾。但是现在人们谈及容灾往往只是针对本地容灾而言的。但对企业来讲，仅有本地容灾是远远不够的，更多的应是异地容灾。因此一套完整的容灾方案应该包括本地容灾系统和异地容灾系统。另外，容灾系统还必须要有有效的管理机制。

4.7.2　数据容灾技术

1. 容灾技术概述

容灾系统的核心技术是数据复制，目前主要有同步数据复制和异步数据复制两种。同步数据复制是指通过将本地生产数据以完全同步的方式复制到异地，每一个本地 I/O 交易均需等待远程复制的完成方予以释放。异步数据复制是指将本地生产数据以后台方式复制到异地，每一个本地 I/O 交易均正常释放，无须等待远程复制的完成。数据复制对数据系统的一致性和可靠性以及系统的应变能力具有举足轻重的作用，它决定着容灾系统的可靠性和可用性。

对数据库系统可采用远程数据库复制技术来实现容灾。这种技术是由数据库系统软件来实现数据库的远程复制和同步的。基于数据库的复制方式可分为实时复制、定时复制和存储转发复制，并且在复制过程中，还有自动冲突检测和解决的手段，以保证数据的一致性不受破坏。远程数据库复制技术对主机的性能有一定影响，可能增加对磁盘存储容量的需求，但系统运行恢复较简单，实时复制方式时数据一致性较好，所以对于一些对数据一



致性要求较高、数据修改更新较频繁的应用，可采用基于数据库的容灾备份方案。

目前，业内实施比较多的容灾技术是基于智能存储系统的远程数据复制技术。它使智能存储系统自身实现数据的远程复制和同步，即智能存储系统将对本系统中的存储器 I/O 操作请求复制到远端的存储系统中并执行，以保证数据的一致性。

还可以采用基于逻辑磁盘卷的远程数据复制技术进行容灾。这种技术就是将物理存储设备划分为一个或者多个逻辑磁盘卷(Volume)，便于数据的存储规划和管理。逻辑磁盘卷可理解为在物理存储设备和操作系统之间增加一个逻辑存储管理层。基于逻辑磁盘卷的远程数据复制是指根据需要将一个或多个卷进行远程同步或异步复制。该方案通常通过软件来实现，基本配置包括卷管理软件和远程复制控制管理软件。由于逻辑磁盘卷的远程数据复制是基于逻辑存储管理技术，一般与主机系统、物理存储系统设备无关，对物理存储系统自身的管理功能要求不高，有较好的可管理性。

在建立容灾备份系统时会涉及多种技术，具体有 SAN 和 NAS 技术、远程镜像技术、虚拟存储技术、基于 IP 的 SAN 的互联技术、快照技术等。

2. SAN 和 NAS 技术

SAN(Storage Area Network，存储区域网)提供一个存储系统、备份设备和服务器相互连接的架构。它们之间的数据不再在以太网上流通，从而大大提高了以太网的性能。正由于存储设备与服务器完全分离，用户获得一个与服务器分开的存储管理理念。复制、备份、恢复数据和安全的管理可以以中央的控制和管理手段进行，加上把不同的存储池以网络方式连接，用户可以以任何需要的方式访问他们的数据，并获得更高的数据完整性。

NAS(Network Attached Storage，网络附加存储)使用了传统以太网和 IP 协议，当进行文件共享时，则利用 NFS 和 CIFS(Common Internet File System)沟通 NT 和 UNIX 系统。由于 NFS 和 CIFS 都是基于操作系统的文件共享协议，所以 NAS 的性能特点是进行小文件级的共享存取。

SAN 以光纤通道交换机和光纤通道协议为主要特征的本质决定了它在性能、距离、管理等方面的诸多优点。而 NAS 的部署非常简单，只需与传统交换机连接即可；NAS 的成本较低，因为它的投资仅限于一台 NAS 服务器，而不像 SAN 是整个存储网络，同时，NAS 服务器的价格往往是针对中小企业定位的；NAS 服务器的管理也非常简单，它一般都支持 Web 的客户端管理，对熟悉操作系统的网络管理人员来说，其设置既熟悉又简单。概括来说，SAN 对于高容量块状级数据传输具有明显的优势，而 NAS 则更加适合文件级别上的数据处理。SAN 和 NAS 实际上也是能够相互补充的存储技术。

SAN 的高可用性是基于它对灾难恢复、在线备份能力和对冗余存储系统和数据的时效切换能力。NAS 应用成熟的网络结构提供快速的文件存取和高可用性、数据复制等功能可以保护和提供稳固的文件级存储。

3. 远程镜像技术

远程镜像技术用在主数据中心和备援数据中心之间的数据备份。两个镜像系统一个叫主镜像系统，另一个叫从镜像系统。按主、从镜像存储系统所处的位置可分为本地镜像和远程镜像。

远程镜像又叫远程复制，是容灾备份的核心技术，同时也是保持远程数据同步和实现

灾难恢复的基础。远程镜像按请求镜像的主机是否需要远程镜像站点的确认信息，又可分为同步远程镜像和异步远程镜像。

同步远程镜像(同步复制技术)是指通过远程镜像软件，将本地数据以完全同步的方式复制到异地，每一个本地的 I/O 事务均需等待远程复制的完成确认信息，方可予以释放。同步镜像使远程复制总能与本地机要求复制的内容相匹配。当主站点出现故障时，用户的应用程序切换到备份的替代站点后，被镜像的远程副本可以保证业务继续执行而没有数据的丢失。但同步远程镜像系统存在往返传输造成延时较长的缺点，因此只限于在相对较近的距离间应用。

异步远程镜像(异步复制技术)保证在更新远程存储视图前完成向本地存储系统的基本 I/O 操作，而由本地存储系统提供完成确认信息给请求镜像主机的 I/O 操作。远程的数据复制是以后台同步方式进行的，这使本地系统性能受到的影响很小，传输距离远(可达 1000km 以上)，对网络带宽要求低。但是，许多远程的从属存储子系统的写操作尚未得到确认，此时某种因素造成数据传输失败时，可能会出现数据的不一致性问题。为了解决这个问题，目前大多采用延迟复制的技术，即在确保本地数据完好无损后进行远程数据更新。

4. 快照技术

远程镜像技术往往同快照技术结合起来实现远程备份，即通过镜像把数据备份到远程存储系统中，再用快照技术把远程存储系统中的信息备份到远程的磁带库、光盘库中。

快照是通过软件对要备份的磁盘子系统的数据快速扫描，建立一个要备份数据的快照逻辑单元号(LUN)和快照 Cache。在快速扫描时，把备份过程中即将要修改的数据块同时快速复制到快照 Cache 中。快照 LUN 是一组指针，它指向快照 Cache 和磁盘子系统中不变的数据块(在备份过程中)。在正常业务进行的同时，利用快照 LUN 实现对原数据的一个完全备份。它可使用户在正常业务不受影响的情况下，实时提取当前在线业务数据。其“备份窗口”接近于零，可大大增加系统业务的连续性，为实现系统真正的 7d×24h 运转提供了保证。

5. 互联技术

早期的主数据中心和备援数据中心之间的数据备份，主要是基于 SAN 的远程复制(镜司像)，即通过光纤通道把两个 SAN 连接起来，进行远程镜像(复制)。当灾难发生时，由备援数据中心替代主数据中心保证系统工作的连续性。这种远程容灾备份方式存在一些缺陷，如实现成本高、设备的互操作性差、跨越的地理距离短(10km)等，这些因素阻碍了它的进一步推广和应用。

目前，出现了多种基于 IP 的 SAN 的远程数据容灾备份技术。它们是利用基于 IP 的 SAN 的互联协议，将主数据中心 SAN 中的信息通过现有的 TCP/IP 网络，远程复制到备援中心 SAN 中。当备援中心存储的数据量过大时，可利用快照技术将其备份到磁带库或光盘库中。这种基于 IP 的 SAN 的远程容灾备份，可以跨越 LAN、MAN 和 WAN，其成本低、扩展性好，具有广阔的发展前景。基于 IP 的互联网协议有 FCIP、iFCP、Infiniband、iSCSI 等。

6. 虚拟存储技术

在有些容灾方案中，还采取了虚拟存储技术，如西瑞异地容灾方案。虚拟化存储技术



在系统弹性和可扩展性方面开创了新的局面。它将几个 IDE 或 SCSI 驱动器等不同的存储设备串联成一个存储器池。存储器池的整个存储容量可以分为多个逻辑卷，并作为虚拟分区进行管理。存储由此成为一种功能而非物理属性，而这正是基于服务器的存储结构存在的主要限制。

虚拟存储系统还提供了动态改变逻辑卷大小的功能。事实上，存储卷的容量可以在线随意增加或减少。可以通过在系统中增加或减少物理磁盘的数量来改变集群中逻辑卷的大小。这一功能允许卷的容量随用户的即时要求而动态改变。另外，存储卷能够很容易地改变容量、移动和替换。安装系统时，只需为每个逻辑卷分配最小的容量，并在磁盘上留出剩余的空间。随着业务的发展，可利用剩余空间根据需要扩展逻辑卷，也可以将数据在线从旧驱动器转移到新的驱动器上，而不中断正常服务的运行。

存储虚拟化的一个关键优势是它允许异构系统和应用程序共享存储设备，而不管它们位于何处。系统将不再需要在每个分部的服务器上都连接一台磁带设备。

复习思考题四

一、填空题

1. 按数据备份时备份的数据不同，可有__________、__________、__________和按需备份等备份方式。

2. 数据恢复操作通常可分为 3 类：__________、__________和重定向恢复。

3. 数据备份是数据容灾的__________。

4. 常见的灾难备份等级有 4 级：第__________级、第__________级、第__________级和第__________级。

5. 数据的__________是指保护网络中存储和传输数据不被非法改变。

6. 数据库安全包括数据库__________安全性和数据库__________安全性两层含义。

7. __________是指在多用户的环境下，对数据库的并行操作进行规范的机制，从而保证数据的正确性与一致性。

8. 当故障影响数据库系统操作，甚至使数据库中数据全部或部分丢失时，希望能尽快恢复到原数据库状态或重建一个完整的数据库，该处理称为__________。

9. __________是指为防止系统出现操作失误或系统故障导致数据丢失，而将全系统或部分数据从主机的硬盘或阵列中复制到其他存储介质上的过程。

10. 影响数据完整性的主要因素有__________、软件故障、__________、人为威胁和意外灾难等。

11.__________是指数据库的任何部分都没受到侵害，或没受到未经授权的存取和修改。

12. 数据的__________就是数据与应用程序之间不存在相互依赖关系，也就是数据的逻辑结构、存储结构和存取方法等不因应用程序的修改而改变，反之亦然。

二、单项选择题

1. 按数据备份时数据库状态的不同有(　　)。

A. 热备份　　B. 冷备份　　C. 逻辑备份　　D. A、B、C 都对

2. 数据库系统的安全框架可以划分为网络系统、(　　)和 DBMS 三个层次。

A. 操作系统　　B. 数据库系统　　C. 软件系统　　D. 容错系统

3. 按备份周期对整个系统所有的文件进行备份的方式是(　　)备份。

A. 完全　　B. 增量　　C. 差别　　D. 按需

4. 在网络备份系统中，(　　)是执行备份或恢复任务的系统，它提供一个集中管理和控制平台，管理员可以利用该平台去配置整个网络备份系统。

A. 目标　　B. 工具　　C. 通道　　D. 存储设备

三、问答题

1. 简述数据库数据的安全措施。
2. 简述数据库系统安全威胁的来源。
3. 什么叫数据库的完整性?数据库的完整性约束条件有哪些?
4. 简述保护数据完整性的容错方法。
5. 什么叫数据备份?数据备份有哪些类型？
6. 什么叫数据容灾？数据容灾技术有哪些?
7. 简要介绍同步远程镜像和异步远程镜像技术。
8. 简要介绍虚拟存储技术。

第 5 章　计算机病毒防治技术

学习目标

系统学习计算机病毒的概念、特点及分类，计算机网络病毒的概念、特点和分类以及计算机网络病毒的危害；学习几种典型病毒的原理及清除方法；了解计算机病毒发作前、发作时和发作后的症状；同时了解反病毒技术、计算机病毒发展的新技术和防杀网络病毒的软件等。通过本章的学习，读者应掌握及了解以下内容。

- 掌握计算机病毒的概念、特点和分类，几种典型病毒的原理、特征及预防措施，计算机病毒的症状，反病毒技术。
- 了解计算机病毒发展的新技术，防杀网络病毒的软件。

5.1　计算机网络病毒的特点及危害

计算机病毒对系统的危害是众所周知的。起初的计算机病毒只是在单机中传播，而如今随着计算机网络应用的日益普及，计算机病毒凭借互联网迅速地传播、繁殖，其速度和危害性已引起越来越多人的重视。目前，在网络信息安全领域，计算机病毒特别是网络病毒已经成为一种有效的攻击手段。

5.1.1　计算机病毒的概念

“计算机病毒”与医学上的“病毒”不同，它是根据计算机软、硬件所固有的弱点，编制出的具有特殊功能的程序。由于这种程序具有传染性和破坏性，与医学上的“病毒”有相似之处，因此习惯上将这些“具有特殊功能的程序”称为“计算机病毒”。

1983 年 11 月 10 日，美国人 Fred Cohen 以测试计算机安全为目的，编写并发布了首个计算机病毒。20 多年后的今天，全世界已约有 6 万种计算机病毒，极大地威胁着计算机信息安全，如 2004 年上半年的“震荡波”病毒横扫全世界。“震荡波”病毒会在网络中自动搜索系统有漏洞的计算机，并引导其下载病毒文件并执行。整个传播和发作过程不需要人为干预，只要这些计算机接入 Internet 且没有安装相应的系统补丁程序，就有可能被感染。病毒会使“安全认证子系统”进程(lsass.exe)崩溃，致使系统反复重启，并且使与安全认证有关的程序出现严重运行错误。

从广义上讲，凡能够引起计算机故障，破坏计算机数据的程序统称为计算机病毒。依据此定义，诸如逻辑炸弹、蠕虫等均可称为计算机病毒。

1994 年 2 月 18 日，我国正式颁布实施《中华人民共和国计算机信息系统安全保护条例》，在该条例的第二十八条中明确指出，计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能，或者毁坏数据、影响计算机使用，并能自我复制的一组计算机指令或者程序代码。此定义具有法律性、权威性。



5.1.2　计算机病毒的特点

1. 传染性

计算机病毒会通过各种渠道从已被感染的计算机扩散到未被感染的计算机，造成被感染的计算机工作失常甚至瘫痪。与生物病毒不同的是，计算机病毒代码一旦进入计算机并执行，它就会搜寻其他符合传染条件的程序或存储介质，确定目标后再将自身代码插入其中，达到自我繁殖的目的。

计算机病毒可以通过各种可能的渠道，如软盘、计算机网络去传染其他的计算机，是否具有传染性是判别一个程序是否为计算机病毒的最重要条件。

病毒具有正常程序的一切特性，它隐藏在正常程序中，当用户调用正常程序时，病毒窃取到系统的控制权，先于正常程序执行，病毒的动作、目的对用户是未知的，是未经用户允许的。

2. 隐蔽性

病毒通常附在正常程序中或磁盘较隐蔽的地方，也有的以隐含文件形式出现，目的是不让用户发现它的存在。如果不经过代码分析，病毒程序与正常程序是不容易区别开来的。在没有防护措施的情况下，受到感染的计算机系统通常仍能正常运行，用户不会感到任何异常。大部分的病毒代码设计得非常短小，一般只有几百字节或 1KB。

计算机病毒的源程序可以是一个独立的程序体，源病毒经过扩散生成的再生病毒往往采用附加和插入的方式隐藏在可执行程序和数据文件中，采取分散和多处隐藏的方式；而当有病毒程序潜伏的程序体被合法调用时，病毒程序也合法进入，并可将分散的程序部分在非法占用的存储空间进行重新装配，构成一个完整的病毒体投入运行。

3. 潜伏性

大部分的病毒感染系统之后长期隐藏在系统中，悄悄地繁殖和扩散而不被发觉，只有在满足其特定条件时才启动其表现(破坏)模块。只有这样它才可达到长期隐藏、偷偷扩散的目的。

4. 破坏性(表现性)

任何病毒只要侵入系统，就会对系统及应用程序产生程度不同的影响。轻则会降低计算机工作效率，占用系统资源；重则可导致系统崩溃。根据病毒的这一特性可将病毒分为良性病毒与恶性病毒。良性病毒可能只显示些画面或无聊的语句，或者根本没有任何破坏动作，但会占用系统资源，这类病毒表现较为温和。恶性病毒则有明确的目的，或破坏数据、删除文件，或加密磁盘、格式化磁盘，甚至造成不可挽回的损失。表现和破坏是病毒的最终目的。

5. 不可预见性

从对病毒的检测方面来看，病毒还有不可预见性。不同种类的病毒，其代码千差万别，但有些操作是共有的(如驻留内存、更改中断等)。有些人利用病毒的这种共性，制作了声称可查所有病毒的程序。这种程序的确可查出一些新病毒，但由于目前的软件种类极多，



且某些正常程序也使用了类似病毒的操作，甚至借鉴了某些病毒技术，因此使用这种方法对病毒进行检测，势必会造成较多的误报情况，而且病毒的制作技术也在不断地提高，病毒对反病毒软件永远是超前的。

6. 触发性

病毒因某个事件或数值的出现，诱使病毒实施感染或进行攻击的特性称为可触发性。病毒既要隐蔽又要维持攻击力，必须具有可触发性。

病毒的触发机制用于控制感染和破坏动作的频率。计算机病毒一般都有一个触发条件，它可以按照设计者的要求在某个点上激活并对系统发起攻击。

病毒的触发条件有以下几种。

(1) 以时间作为触发条件。计算机病毒程序读取系统内部时钟，当满足设计的时间时开始发作。

(2) 以计数器作为触发条件。计算机病毒程序内部设定一个计数单元，当满足设计者的特定值时就发作。

(3) 以特定字符作为触发条件。当敲入某些特定字符时即发作。

(4) 组合触发条件。综合以上几个条件作为计算机病毒的触发条件。

病毒中有关触发机制的编码是其敏感部分。剖析病毒时，如果清楚病毒的触发机制，就可以修改此部分代码，使病毒失效，也可以产生没有潜伏性的极为外露的病毒样本，供反病毒研究用。满足传染触发条件时，病毒的传染模块会被激活，实施传染操作。满足表现触发条件时，病毒的表现模块会被激活，实施表现或破坏操作。

7. 针对性

病毒的触发有一定的环境要求，并不一定对任何系统都能感染。

8. 寄生性(依附性)

计算机病毒程序嵌入到宿主程序中，依赖于宿主程序的执行而生存，这就是计算机病毒的寄生性。病毒程序在侵入到宿主程序中后，一般会对宿主程序进行一定的修改，宿主程序一旦执行，病毒程序就会被激活，从而可以进行自我复制。

通常认为，计算机病毒的主要特点是传染性、隐蔽性、潜伏性、寄生性和破坏性。

5.1.3　计算机病毒的分类

按照计算机病毒的特点，对计算机病毒可从不同角度进行分类。计算机病毒的分类方法有许多种，因此，同一种病毒可能有多种不同的分类方法。

1. 基于破坏程度分类

基于破坏程度分类是最流行、最科学的分类方法之一，按照此种分类方法，病毒可以分为良性病毒和恶性病毒。

(1) 良性病毒是指其中不含有立即对计算机系统产生直接破坏作用的代码。这类病毒为了表现其存在，只是不停地进行扩散，从一台计算机传染到另一台，虽然不破坏计算机内的数据，却会造成计算机程序的工作异常。

良性病毒取得系统控制权后，会导致整个系统运行效率降低、可用内存容量减少、某些应用程序不能运行，还与操作系统和应用程序争抢 CPU 的控制权，有时还会导致整个系统死锁，给正常操作带来麻烦。有时系统内还会出现几种病毒交叉感染的现象，即一个文件不停地反复被几种病毒所感染。常见的良性病毒有“小球”病毒、“台湾一号”、“维也纳”和“巴基斯坦”病毒等。

(2) 恶性病毒在其代码中包含有破坏计算机系统的操作，在其传染或发作时会对系统产生直接的破坏作用。恶性病毒感染后一般没有异常表现，会将自己隐藏得更深，但是一旦发作，就会破坏计算机数据、删除文件，有的甚至会对硬盘进行格式化，造成整个计算机系统瘫痪，等人们察觉时，已经对计算机数据或硬件造成了破坏，损失将难以挽回。

这种病毒有很多，如“黑色星期五”、“CIH 系统毁灭者”等。恶性病毒是很危险的，应当注意防范。

2. 基于传染方式分类

按照传染方式不同，病毒可分为引导型病毒、文件型病毒和混合型病毒 3 种。

(1) 引导型病毒是指开机启动时，病毒在 DOS 的引导过程中被载入内存，它先于操作系统运行，所依靠的环境是 BIOS 中断服务程序。引导区是磁盘的一部分，它在开机启动时控制计算机系统。引导型病毒正是利用了操作系统的引导区位置固定，且控制权的转交方式以物理地址为依据，而不是以引导区的内容为依据这一特点，将真正的引导区内容进行转移或替换，待病毒程序被执行后，再将控制权交给真正的引导区内容，使得这个带病毒的系统看似正常运转，而病毒已隐藏在系统中等待时机传染和发作。

引导型病毒按其寄生对象的不同，又可分为主引导区病毒和引导区病毒。主引导区病毒又称分区病毒，此病毒寄生在硬盘分区主引导程序所占据的硬盘 0 磁头 0 柱面第 1 个扇区中，如 Stoned 病毒。引导区病毒是将病毒寄生在硬盘逻辑 0 扇区或软盘逻辑 0 扇区，典型的如小球病毒。它们的原理基本相同，在这里只介绍引导区病毒。

引导型病毒通常分为两部分，一部分放在磁盘引导区中；另一部分和原引导记录放在磁盘上连续几个簇中，这些簇在文件分配表(FAT)中做上坏簇的标记，使其不被覆盖而永久地驻留在磁盘中。开机启动时，磁盘引导区的程序会读入内存中，引导程序得到控制权后会加载两个隐含文件，即 ibmbio.com 和 command.com 以完成启动。如果是染上病毒的盘，读入内存的则是病毒程序的第一部分，它得到控制权后修改内存可用空间的大小，在内存高端开辟出一块区域，并把第一部分移至该区域；接着读入放在磁盘坏簇中的第二部分，并和第一部分拼起来，使病毒程序全部驻留在内存的高端，以防在运行其他程序时被覆盖；然后修改 INT13H 的中断向量或其他中断向量，使其指向病毒程序，这时才把原引导程序读入内存中，并把控制权交由它来完成系统的启动。由于修改了中断向量，病毒程序在计算机的运行中经常能得到 CPU 的控制权，这样在读写盘或产生其他中断时，病毒就可以发作进行破坏了。

(2) 文件型病毒依靠可执行文件，即文件扩展名为.com 和.exe 等程序，它们存放在可执行文件的头部或尾部。目前绝大多数的病毒都属于文件型病毒。

文件型病毒将其代码加载到运行程序的文件中，只要运行该程序，病毒就会被激活，引入内存，并占领 CPU 得到控制权。病毒会在磁盘中寻找未被感染的可执行文件，将自身



放入其首部或尾部，并修改文件的长度使病毒程序合法化，它还能修改该程序，使该文件执行前首先挂靠病毒程序，在病毒程序的出口处再跳向源程序开始处，这样就使该执行文件成为新的病毒源。已感染病毒的文件执行速度会减缓，甚至完全无法执行，也有些文件遭感染后，一执行就会被删除。

文件型病毒依附在不可执行的文件中是没有意义的，只有运行可执行程序时病毒才能调入内存运行。

文件型病毒按照传染方式的不同，又可分为非常驻型、常驻型和隐形文件型 3 种。

① 非常驻型病毒：非常驻型病毒将自己寄生在.com，.exe 或是.sys 的文件中，当执行感染病毒的程序时，该病毒就会传染给其他文件。

② 常驻型病毒：常驻型病毒躲藏在内存中，会对计算机造成更大的伤害，一旦它进入内存中，只要文件被执行，它就会迅速感染其他文件。

③ 隐形文件型病毒：把自己植入操作系统里，当程序向操作系统要求中断服务时，它就会感染这个程序，而且没有任何表现。

引导型病毒破坏性较大，但数量较少，直到 20 世纪 90 年代中期，文件型病毒还是最流行的病毒。随着微软公司 Word 字处理软件的广泛使用以及 Internet 的推广普及，又出现一种新病毒，这就是宏病毒。宏病毒可算作文件型病毒的一种。宏病毒已占目前全部病毒数量的 80%以上，它是发展最快的病毒。宏病毒还可衍生出各种变种病毒。

(3) 混合型病毒通过技术手段把引导型病毒和文件型病毒组合成为一体，使之具有引导型病毒和文件型病毒两种特征，以两者相互促进的方式进行传染。这种病毒既可以传染引导区又可以传染可执行文件，增加了病毒的传染性及存活率。不管以哪种方式传染，只要进入计算机就会经开机或执行程序而感染其他的磁盘或文件，从而使其传播范围更广，更难以被清除干净。如果只将病毒从被感染的文件中清除掉，当系统重新启动时，病毒又将从硬盘引导记录进入内存，文件被重新感染；如果只将隐藏在引导记录里的病毒消除掉，当运行文件时，引导记录又会被重新感染。

3. 基于算法分类

按照病毒特有的算法，可以划分为伴随型病毒、蠕虫型病毒和寄生型病毒。

(1) 伴随型病毒。它并不改变文件本身，而是根据算法产生.exe 文件的伴随体，与文件具有同样的名字和不同的扩展名，例如 ccr.exe 的伴随体是 ccr.com。当 DOS 加载文件时，伴随体优先被执行，再由伴随体加载执行原来的.exe 文件。

(2) 蠕虫型病毒。通过计算机网络进行传播，它不改变文件和资料信息，而是根据计算机的网络地址，将病毒通过网络发送，蠕虫病毒除了占用内存外一般不占用其他资源。

(3) 寄生型病毒。除伴随型病毒和蠕虫型病毒之外的其他病毒均可称为寄生型病毒。它们依附在系统的引导区或文件中，通过系统的功能进行传播，按算法又可分为练习型病毒、诡秘型病毒和变型病毒。

① 练习型病毒自身包含错误，不能很好地传播，如一些处在调试阶段的病毒。

② 诡秘型病毒一般不直接修改 DOS 中断和扇区数据，而是通过设备技术和文件缓冲区等进行 DOS 内部修改，由于该病毒使用比较高级的技术，所以不易清除。

③ 变型病毒又称幽灵病毒，这种病毒使用较复杂的算法，使自己每传播一份都具有



不同的内容和长度。它们通常由一段混有无关指令的解码算法和变化过的病毒体组成。

4. 基于链接方式分类

按照病毒的链接方式，可以分为源码型病毒、入侵型病毒、外壳型病毒和操作系统型病毒。

(1) 源码型病毒攻击的目标是源程序。在源程序编译之前，将病毒代码插入源程序，编译后，病毒变成合法程序的一部分，成为以合法身份存在的非法程序。

源码型病毒比较少见，在编写时要求源码病毒所用语言必须与被攻击源码程序的语言相同。

(2) 入侵型病毒可用自身代替宿主程序中的部分模块或堆栈区，因此这类病毒只攻击某些特定程序，针对性强。这种病毒的编写也很困难，因为病毒遇见的宿主程序千变万化，病毒在不了解其内部逻辑的情况下，要将宿主程序拦腰截断，插入病毒代码，而且还要保证病毒程序能正常运行。该病毒一旦侵入程序体后也较难消除。如果同时采用多态性病毒技术、超级病毒技术和隐蔽性病毒技术，将给当前的反病毒技术带来严峻的挑战。

(3) 外壳型病毒将其自身附在宿主程序的头部或尾部，相当于给宿主程序增加了一个外壳，但对宿主程序不作修改。这种病毒最为常见，易于编写，也易于被发现，通过测试文件的大小即可发现。大部分的文件型病毒都属于这一类。

(4) 操作系统型病毒用它自己的程序加入或取代部分操作系统进行工作，具有很强的破坏力，可以导致整个系统瘫痪。圆点病毒和大麻病毒就是典型的操作系统型病毒。这种病毒在运行时，用自己的逻辑部分取代操作系统的合法程序模块，对操作系统进行破坏。

5. 基于传播的媒介分类

按照病毒传播的媒介，可以分为网络病毒和单机型病毒。

(1) 网络病毒通过计算机网络传播感染网络中的可执行文件。这种病毒的传染能力强，破坏力大。

(2) 单机型病毒的载体是磁盘，常见的是病毒从软盘传入硬盘，感染系统，然后再传染其他软盘，再由软盘传染其他系统。

6. 基于攻击的系统分类

按照计算机病毒攻击的系统，可以分为攻击 DOS 系统的病毒、攻击 Windows 系统的病毒、攻击 UNIX 系统的病毒和攻击 OS/2 系统的病毒。

(1) 攻击 DOS 系统的病毒。这类病毒出现最早、数量最大，变种也最多，以前计算机病毒基本上都是这类病毒。

(2) 攻击 Windows 系统的病毒。Windows 因其图形用户界面和多任务操作系统而深受用户的欢迎，Windows 现已逐渐取代 DOS，从而成为病毒攻击的主要对象。我国发现的首例破坏计算机硬件的 CIH 病毒就是一个 Windows 95/98 病毒。

(3) 攻击 UNIX 系统的病毒。UNIX 系统应用非常广泛，并且许多大型的操作系统均采用 UNIX 作为其主要的操作系统，所以 UNIX 病毒的出现，对信息处理也是一个严重的威胁。

(4) 攻击 OS/2 系统的病毒。世界上已经发现第一个攻击 OS/2 系统的病毒。



7. 基于激活的时间分类

按照病毒激活的时间，可分为定时病毒和随机病毒。

定时病毒仅在某一特定时间才发作；而随机病毒一般不是由时钟来激活的。

上述分类是相对的，同一种病毒按不同的分类方法可属于不同类型。

5.1.4 计算机网络病毒的概念

1. 计算机网络病毒的定义

传统的网络病毒是指利用网络进行传播的一类病毒的总称。网络成了传播病毒的通道，使病毒从一台计算机传染到另一台计算机，然后传遍网络中的全部计算机，一般如果发现网络中有一个站点感染病毒，那么其他站点也会有类似病毒。一个网络系统只要有入口点，那么就很有可能感染上网络病毒，使病毒在网络中传播扩散，甚至会破坏整个系统。

严格地说，网络病毒是以网络为平台，能在网络中传播、复制及破坏的计算机病毒，像网络蠕虫病毒等一些威胁到计算机及计算机网络正常运行和安全的病毒才可以算作计算机网络病毒。“网络病毒”与单机病毒有较大区别。计算机网络病毒专门使用网络协议(如TCP/IP、FTP、UDP、HTTP、SMTP 和 POP3 等)来进行传播，它们通常不修改系统文件或硬盘的引导区，而是感染客户计算机的内存，强制这些计算机向网络发送大量信息，因而导致网络速度下降甚至完全瘫痪。由于网络病毒保留在内存中，因此传统的基于磁盘的文件 I/O 扫描方法通常无法检测到它们。

2. 计算机网络病毒的传播方式

Internet 技术的进步同样给许多恶毒的网络攻击者提供了一条便捷的攻击路径，他们利用网络来传播病毒，其破坏性和隐蔽性更强。

一般来说，计算机网络的基本构成包括网络服务器和网络节点(包括有盘工作站、无盘工作站和远程工作站)。病毒在网络环境下的传播，实际上是按照“工作站—服务器—工作站”的方式进行循环传播。计算机病毒一般先通过有盘工作站的软盘或硬盘进入网络，然后开始在网络中传播。

具体地说，其传播方式有以下几种。

(1) 病毒直接从有盘工作站复制到服务器中。

(2) 病毒先感染工作站，在工作站内存驻留，等运行网络盘内程序时再感染服务器。

(3) 病毒先感染工作站，在工作站内存驻留，当病毒运行时通过映像路径感染到服务器中。

(4) 如果远程工作站被病毒侵入，病毒也可以通过通信中数据的交换进入网络服务器中。

计算机网络病毒的传播和攻击主要通过两个途径，即用户邮件和系统漏洞。所以，一方面，网络用户要加强自身的网络意识，对陌生的电子邮件和网站提高警惕；另一方面，操作系统要及时地进行系统升级，以加强对病毒的防范能力。

随着 Internet 的发展，病毒的传播速度明显加快，传播范围也开始从区域化走向全球化。新一代病毒主要通过电子邮件、网页浏览、网络服务等网络途径传播，传播速度更快、发



生频率更高，防御更困难，往往在找到解决办法前，病毒已经造成严重危害。

5.1.5　计算机网络病毒的特点

从计算机网络病毒的传播方式可以看出，计算机网络病毒除具有一般病毒的特点外，还有以下新的特点。

1. 传染方式多

病毒入侵网络系统的主要途径是通过工作站传播到服务器硬盘，再由服务器的共享目录传播到其他工作站。但病毒传染方式比较复杂，通常有以下几种。

(1)　引导型病毒对工作站或服务器的硬盘分区表或 DOS 引导区进行传染。

(2)　通过在有盘工作站上执行带毒程序，而传染服务器映射盘上的文件。由于 login.exe 文件是用户入网登录时第一个被调用的可执行文件，因此该文件最易被病毒感染，而 login.exe 文件一旦被病毒感染，则每个工作站在使用其登录时便会被感染，并进一步感染服务器共享目录。

(3)　服务器上的程序若被病毒感染，则所有使用该带毒程序的工作站都将被感染。混合型病毒有可能感染工作站上的硬盘分区表或 DOS 引导区。

(4)　病毒通过工作站的复制操作进入服务器，进而在网上传播。

(5)　利用多任务可加载模块进行传染。

(6)　若 Novell 服务器的 DOS 分区程序 server.exe 已被病毒感染，则文件服务器系统有可能被感染。

2. 传播速度快

单机病毒只能通过磁盘从一台计算机传染到另一台计算机，而网络病毒则可以通过网络通信机制，借助高速电缆迅速扩散。

由于病毒在网络中传播速度非常快，故其扩散范围很大。根据测定，PC 网络在正常使用情况下，只要有一台工作站有病毒，就可在几十分钟内将网上的数百台计算机全部感染。

3. 清除难度大

再顽固的单机病毒也可通过删除带毒文件、格式化硬盘等措施将病毒清除，而网络中只要有一台工作站中还有病毒未杀干净，就可使整个网络全部重新被病毒感染，甚至刚刚完成杀毒工作的一台工作站也有可能被网上另一台工作站的带毒程序所传染。因此，仅对工作站进行杀毒处理并不能彻底解决网络病毒问题。

4. 扩散面广

由于病毒在网络中扩散非常快，扩散范围很大，不但能迅速传染局域网内所有计算机，还能通过远程工作站将病毒在一瞬间传播到千里之外。

5. 破坏性大

网络上的病毒将直接影响网络的工作，轻则降低速度，影响工作效率；重则造成网络系统瘫痪，破坏服务器系统资源，使众多工作毁于一旦。



5.1.6 计算机网络病毒的分类

计算机网络病毒的发展是相当迅速的，目前主要的网络病毒有以下几种。

1. 网络木马病毒

传统的木马病毒(Trojan)是指一些有正常程序外表的病毒程序，如一些密码窃取病毒，它会伪装成系统登录框，当在登录框中输入用户名与密码时，这个伪装登录框的木马便会将用户口令通过网络泄露出去。

2. 蠕虫病毒

蠕虫病毒(Worm)是指利用网络缺陷进行繁殖的病毒程序，如“莫里斯”病毒就是典型的蠕虫病毒。它利用网络的缺陷在网络中大量繁殖，导致几千台服务器无法正常提供服务。如今的蠕虫病毒除了利用网络缺陷外，更多地利用了一些新的技术，例如，“求职信”病毒是利用邮件系统这一大众化的平台，将自己传遍千家万户；“密码”病毒是利用人们的好奇心理，诱使用户主动运行病毒；“尼姆达”病毒则是综合了系统病毒的方法，利用感染文件来加速自己的传播。目前常说的网络病毒就是指蠕虫病毒。

3. 捆绑器病毒

捆绑器病毒(Binder)是一个很新的概念，人们编写这种程序的最初目的是希望通过一次点击可以同时运行多个程序，然而这一工具却成了病毒传播的新帮凶。比如，用户可以将一个小游戏与病毒通过捆绑器程序捆绑，当用户运行游戏时，病毒也会同时悄悄地运行，给用户的计算机造成危害。此外，目前一些图片文件也可以被捆绑病毒，其隐蔽性更高。

4. 网页病毒

网页病毒是利用网页中的恶意代码来进行破坏的病毒。它存在于网页中，其实就是利用一些脚本语言编写的一些恶意代码。它可以对系统的一些资源进行破坏，轻则修改用户的注册表，使用户的首页、浏览器标题改变；重则可以关闭系统的很多功能，使用户无法正常使用计算机；更有甚者则将用户的磁盘进行格式化。这种网页病毒容易编写和修改，使用户防不胜防，最好的方法是选用有网页监控功能的杀毒软件以防万一。

5. 手机病毒

简单地说，手机病毒就是以手机为感染对象，以手机网络和计算机网络为平台，通过病毒短信等形式对手机进行攻击，造成手机异常的一种新型病毒。

随着智能手机的出现，手机本身通过网络可以完成很多原本由计算机才能完成的工作，如信息处理、收发 E-mail 及网页浏览等。为完成这些工作，手机除了硬件设备以外，还需要上层软件的支持。这些上层软件一般是用 Java、C++等语言开发的，是嵌入式操作系统(即把操作系统固化在芯片中)，这就相当于一部小型计算机，因此，肯定会有受到恶意代码攻击的可能。而目前的短信并不只是简单的文本内容，也包括手机铃声、图片等信息，都需要手机操作系统“翻译”以后再使用。目前的恶意短信就是利用了这个特点，编制出针对某种手机操作系统漏洞的短信内容，攻击手机。如果编制者的水平足够高，对手机的底层

操作系统足够熟悉，他们甚至能编制出毁掉手机芯片的病毒，使手机彻底报废。因此，对手机病毒的危害性不能低估。

手机病毒其实也和计算机病毒一样，可以通过计算机执行从而向手机乱发短信息。严格地讲，手机病毒应该是一种计算机病毒，这种病毒只能在计算机网络中进行传播而不能通过手机进行传播，因此手机病毒其实是计算机病毒程序启动了电信公司的一项服务，如发送电子邮件到手机，而且它发给手机的是文档，根本无破坏力可言。当然，有的手机病毒的破坏力还是比较大的，一旦发作可能比个人计算机病毒更厉害，其传播速度甚至会更快。

黑客如果对手机进行攻击，通常有 3 种表现方式：一是攻击 WAP 服务器使 WAP 手机无法接收正常信息；二是攻击、控制“网关”，向手机发送垃圾信息；三是直接攻击手机本身，使手机无法提供服务，这种破坏方式难度相对较大，目前的技术水平还很难达到。为防范手机病毒，应该尽量少从网上下载信息，平时注意短信息中可能存在的病毒，也可以对手机进行查杀病毒。

目前应对手机病毒的主要技术措施有两种：一是通过无线网站对手机进行杀毒；二是通过手机的 IC 接入口或红外传输口进行杀毒。

在新型网络环境下，滋生了许多新概念病毒，新时代下的计算机病毒越来越“智能”。针对这种状况，除了需要反病毒技术的不断提高外，还需要计算机用户提高防范病毒的意识，只有大家共同努力，才可能有效地遏制病毒的破坏。

5.1.7　计算机网络病毒的危害

在现阶段，由于计算机网络系统的各个组成部分、接口以及各连接层次的相互转换环节都不同程度地存在着某些漏洞和薄弱环节，而网络软件方面的保护机制也不完善，使得病毒通过感染网络服务器，进而在网络上快速蔓延，并影响到各网络用户的数据安全以及计算机的正常运行。一些良性病毒不直接破坏正常代码，只是为了表示它的存在，可能会干扰屏幕的显示，或使计算机的运行速度减慢。一些恶性病毒会明确地破坏计算机的系统资源和用户信息，造成无法弥补的损失。所以计算机网络一旦染上病毒，其影响要远比单机染毒更大，破坏性也更大。

计算机网络病毒的具体危害主要表现在以下几个方面。

(1)　病毒发作对计算机数据信息的直接破坏。大部分病毒在发作时直接破坏计算机的重要信息数据，所利用的手段有格式化磁盘、改写文件分配表和目录区、删除重要文件或者用无意义的“垃圾”数据改写文件以及破坏 CMOS 设置等。

(2)　占用磁盘空间和对信息的破坏。寄生在磁盘上的病毒总要非法占用一部分磁盘空间。引导型病毒是由病毒本身占据磁盘引导扇区，而把原来的引导区转移到其他扇区，被覆盖的扇区数据永久性丢失，无法恢复。文件型病毒利用一些 DOS 功能进行传染，这些 DOS 功能可以检测出磁盘的未用空间，把病毒的传染部分写到磁盘的未用空间去，所以一般不破坏磁盘上的原有数据，只是非法侵占了磁盘空间。一些文件型病毒传染速度很快，在短时间内感染大量文件，每个文件都不同程度地加长了，造成磁盘空间的严重浪费。

(3)　抢占系统资源。除极少数病毒外，大多数病毒在活动状态下都是常驻内存的，这就必然会抢占一部分系统资源。病毒所占用的内存长度大致与病毒本身长度相当。病毒抢



占内存，导致内存减少，会使一部分较大的软件不能运行。此外，病毒还抢占中断，计算机操作系统的很多功能是通过中断调用技术来实现的，病毒为了传染发作，总是修改一些有关的中断地址，从而干扰系统的正常运行。网络病毒会占用大量的网络资源，使网络通信变得极为缓慢，甚至无法使用。

(4) 影响计算机运行速度。病毒进驻内存后不但干扰系统运行，还影响计算机运行速度，主要表现在，病毒为了判断传染发作条件，总要对计算机的工作状态进行监视，这对于计算机的正常运行既多余又有害。有些病毒为了保护自己，不但对磁盘上的静态病毒加密，而且进驻内存后的动态病毒也处在加密状态，CPU 每次寻址到病毒处都要运行一段解密程序把加密的病毒解密成合法的 CPU 指令再执行；而病毒运行结束时再用一段程序对病毒重新加密，这样 CPU 要额外执行数千条甚至上万条指令。另外，病毒在进行传染时同样要插入非法的额外操作，特别是传染软盘时不但使计算机速度明显变慢，而且软盘正常的读写顺序也会被打乱，发出刺耳的噪声。

(5) 计算机病毒错误与不可预见的危害。计算机病毒与其他计算机软件的区别是病毒的无责任性。编制一个完善的计算机软件需要耗费大量的人力、物力，经过长时间调试测试。而病毒都是个别人在一台计算机上匆匆编制调试后就向外抛出。反病毒专家在分析大量病毒后发现，绝大部分病毒都存在不同程度的错误。

(6) 病毒的另一个主要来源是变种病毒。有些计算机初学者尚不具备独立编制软件的能力，出于好奇修改别人的病毒，生成变种病毒，其中就隐含着很多错误。计算机病毒错误所产生的后果往往是不可预见的，有可能比病毒本身的危害还要大。

(7) 计算机病毒给用户造成严重的心理压力。据有关计算机销售部门统计，用户怀疑“计算机有病毒”而提出咨询约占售后服务工作量的 60%以上。经检测确实存在病毒的约占 70%，另有 30%的情况只是用户怀疑有病毒。那么用户怀疑有病毒的理由是什么呢？多半是出现诸如计算机死机、软件运行异常等现象。这些现象确实很有可能是计算机病毒造成的，但又不全是。实际上在计算机工作异常的时候很难要求一位普通用户去准确判断是否是病毒所为。大多数用户对病毒采取宁可信其有的态度，这对于保护计算机安全无疑是十分必要的，然而往往要付出时间、金钱等代价。另外，仅仅因为怀疑有病毒而格式化磁盘所带来的损失更是难以弥补。

总之，计算机病毒像幽灵一样笼罩在广大计算机用户的心头，给人们造成巨大的心理压力，极大地影响了计算机的使用效率，由此带来的无形损失是难以估量的。

5.2 几种典型病毒的分析

计算机病毒有几万种，本节介绍几种典型的计算机病毒。

5.2.1 CIH 病毒

1. CIH 病毒简介

CIH 病毒是我国台湾省一位名叫陈盈豪(CIH 是其名字的缩写)的大学生编写的。目前传播的主要途径是 Internet 和电子邮件。

CIH 病毒属于文件型病毒，主要感染 Windows 9X 下的可执行文件。CIH 病毒使用了面向 Windows 的 VxD 技术，使得这种病毒传播的实时性和隐蔽性都很强。

CIH 病毒至少有 v1.0、v1.1、v1.2、v1.3、v1.4 等 5 个版本。v1.0 版本是最初的 CIH 版本，不具有破坏性；v1.1 版本能自动判断运行系统，如是 Windows NT，则自我隐藏，被感染的文件长度并不增加；v1.2 版本增加了破坏用户硬盘及 BIOS 的代码，成为恶性病毒，发作日是每年 4 月 26 日；v1.3 版本发作日是每年 6 月 26 日；v1.4 版本发作日为每月 26 日。

2. CIH 病毒的破坏性

CIH 病毒感染 Windows 可执行文件，却不感染 Word 和 Excel 文档；感染 Windows 9X 系统，却不感染 Windows NT 系统。

CIH 病毒采取一种特殊的方式对可执行文件进行感染，感染后的文件大小没有变化，病毒代码的大小在 1KB 左右。当一个已染毒的 exe 文件被执行时，CIH 病毒驻留内存，在其他程序访问时对它们进行感染。

CIH 最大的特点就是对计算机硬盘及 BIOS 具有超强的破坏能力。在病毒发作时，病毒从硬盘主引导区开始依次往硬盘中写入垃圾数据，直到硬盘数据全被破坏为止。因此，当 CIH 被发现时，硬盘数据已经遭到破坏，当用户想到要采取措施时，面临的可能已经是一台瘫痪的计算机了。

CIH 病毒发作时还试图覆盖 BIOS 中的数据。一旦 BIOS 被覆盖掉，机器将不能启动，只有对 BIOS 进行重写。

3. 判断感染 CIH 病毒的方法

有两种简单的方法可以判断是否已经感染上了 CIH 病毒。

(1) 一般来讲，CIH 病毒只感染.exe 可执行文件，可以用 Ultra Edit 打开一个常用的.exe 文件(如记事本 NotePad.exe 或写字板 WordPad.exe)，然后单击“切换十六进制模式按钮(H)”，再查找“CIHvl. ”，如果发现“CIHvl.2”、“CIHvl.3”或“CIHvl.4”等字符串，则说明计算机已经感染 CIH 病毒了。

(2) 感染了 CIH v1.2 版，则所有 WinZip 自解压文件均无法自动解开，同时会出现信息“WinZip 自解压首部中断。可能原因：磁盘或文件传输错误。”感染了 CIHvl.3 版，则部分 WinZip 自解压文件无法自动解开。如果遇到以上情况，有可能已感染上 CIH 病毒了。

4. 防范 CIH 病毒的措施

首先应了解 CIH 病毒的发作时间，如每年的 4 月 26 日、6 月 26 日及每月 26 日。在病毒爆发前夕，提前进行查毒、杀毒，同时将系统时间改为其后的时间，如 27 日。

其次，杜绝使用盗版软件，尽量使用正版杀毒软件，并在更新系统或安装新的软件前，对系统或新软件进行一次全面的病毒检查，做到防患于未然。

最后，一定要对重要文件经常进行备份，万一计算机被病毒破坏还可以及时恢复。

5. 感染了 CIH 病毒的处理

首先，注意保护主板的 BIOS。应了解自己计算机主板的 BIOS 类型，如果是不可升级的，用户不必惊慌，因为 CIH 病毒对这种 BIOS 的最大危害，就是使 BIOS 返回到出厂时



的设置，用户只要将 BIOS 重新设置即可。如果 BIOS 是可升级的，用户就不要轻易地从 C 盘重新启动计算机(否则 BIOS 就会被破坏)，而应及时地进入 BIOS 设置程序，将系统引导盘设置为 A 盘，然后用 Windows 的系统引导软盘启动系统到 DOS 7. 0，对硬盘进行一次全面查毒。

由于 CIH 病毒主要感染可执行文件，不感染其他文件，因此用户在彻底清除硬盘所有的 CIH 病毒后，应该重新安装系统软件和应用软件。

最后，如果硬盘数据遭到破坏，可以直接使用瑞星等杀毒软件来恢复。用瑞星杀毒软件软盘来启动计算机，进入瑞星杀毒软件 DOS 版界面，选择【实用工具】菜单中的【修复硬盘数据】命令，根据提示操作，就可以对硬盘进行恢复。恢复完毕后，重启计算机，数据将会失而复得。也可以登录瑞星网站 http://www.rising.com.on 下载硬盘修复专用工具完成数据的恢复。

5.2.2　宏病毒

1. 宏病毒简介

宏病毒是一种使用宏编程语言编写的病毒，主要寄生于 Word 文档或模板的宏中。一旦打开这样的文档，宏病毒就会被激活，进入计算机内存，并驻留在 Normal 模板上。从此以后，所有自动保存的文档都会感染上宏病毒，如果网上其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上。

宏病毒通常使用 VB 脚本影响微软的 Office 组件或类似的应用软件，其大多通过邮件传播。最有名的例子是 1999 年的美丽杀手病毒(Melissa)，通过 Outlook 把自己放在电子邮件的附件中自动寄给其他收件人。

2. 宏病毒的特点

(1)　感染数据文件。以往病毒只感染程序，不感染数据文件，而宏病毒专门感染数据文件，彻底改变了人们的“数据文件不会传播病毒”的认识。

(2)　多平台交叉感染。宏病毒冲破了以往病毒在单一平台上传播的局限。当 Word、Excel 这类著名应用软件在不同平台(如 Windows、OS/2 和 Macintosh)上运行时，会被宏病毒交叉感染。

(3)　容易编写。以往病毒是以二进制的机器码形式出现的，而宏病毒则是以人们容易阅读的源代码形式出现，所以编写和修改宏病毒比以往更容易。这也是前几年宏病毒的数量居高不下的原因。

(4)　容易传播。只要一打开带有宏病毒的电子邮件，计算机就会被宏病毒感染。此后，打开或新建文件都可能染上宏病毒，这导致了宏病毒的感染率非常高。

3. 宏病毒的预防

防治宏病毒的根本措施在于限制宏的执行。以下是一些行之有效的方法。

(1)　禁止所有自动宏的执行。在打开 Word 文档时，按住 Shift 键，即可禁止自动宏，从而达到防治宏病毒的目的。

(2)　检查是否存在可疑的宏。当怀疑系统带有宏病毒时，首先应检查是否存在可疑的

宏，特别是一些奇怪名字的宏肯定是病毒无疑，将它删除即可。即使删除错了，也不会对 Word 文档内容产生任何影响，仅仅是少了相应的“宏功能”而已。具体做法是，选择【工具】菜单中的【宏】命令，打开【宏】对话框，选择要删除的宏，单击【删除】按钮即可。

(3)　按照自己的习惯设置。针对宏病毒感染 Normal.dot 模板的特点，可重新安装 Word 后，建立一个新文档，将 Word 的工作环境按照自己的使用习惯进行设置，并将需要使用的宏一次编制好，做完后保存新文档。这时生成的 Normal.dot 模板绝对没有宏病毒，可将其作备份。在遇到有宏病毒感染时，用备份的 Normal.dot 模板覆盖当前的模板，消除宏病毒。

(4)　使用 Windows 自带的写字板。在使用可能有宏病毒的 Word 文档时，先用 Windows 自带的写字板打开文档，将其转换为写字板格式的文件保存后，再用 Word 调用。因为写字板不调用、不保存任何宏，文档经过这样的转换，所有附带的宏(包括宏病毒)都将丢失，这条经验特别有用。

(5)　提示保存 Normal 模板。大部分 Word 用户仅使用普通的文字处理功能，很少使用宏编程，对 Normal.dot 模板很少去进行修改。因此，可以选择【工具】|【选项】命令，打开【保存】选项卡，选中【提示保存 Normal 模板】复选框。一旦宏病毒感染了 Word 文档，退出 Word 时，Word 就会出现【更改的内容会影响到公用模板 Normal，是否保存这些修改内容？】的提示信息，此时应单击【否】按钮，退出后进行杀毒。

(6)　使用.rtf 和.csv 格式代替.doc 和.xls。要想应付宏所产生的问题，可以使用.rtf 格式的文档来代替.doc 格式，用.csv 格式的电子表格来代替.xls 格式，因为这些格式不支持宏功能。在与其他人交换文件时，使用.rtf 和.csv 格式的文件最安全。

4. 宏病毒的清除

1)　手工清除

【例 5.1】　以 Word 为例，介绍宏病毒的清除操作。

(1)　选择【工具】|【宏】命令，打开宏对话框，如图 5.1 所示。

(2)　单击【管理器】按钮，打开【管理器】对话框，切换到【宏方案项】选项卡，在【宏方案项的有效范围】下拉列表框中选择要检查的文档。这时在上面的列表框中就会出现该文档模板中所含的宏，将不明来源的宏删除，如图 5.2 所示。



图 5.1　【宏】对话框

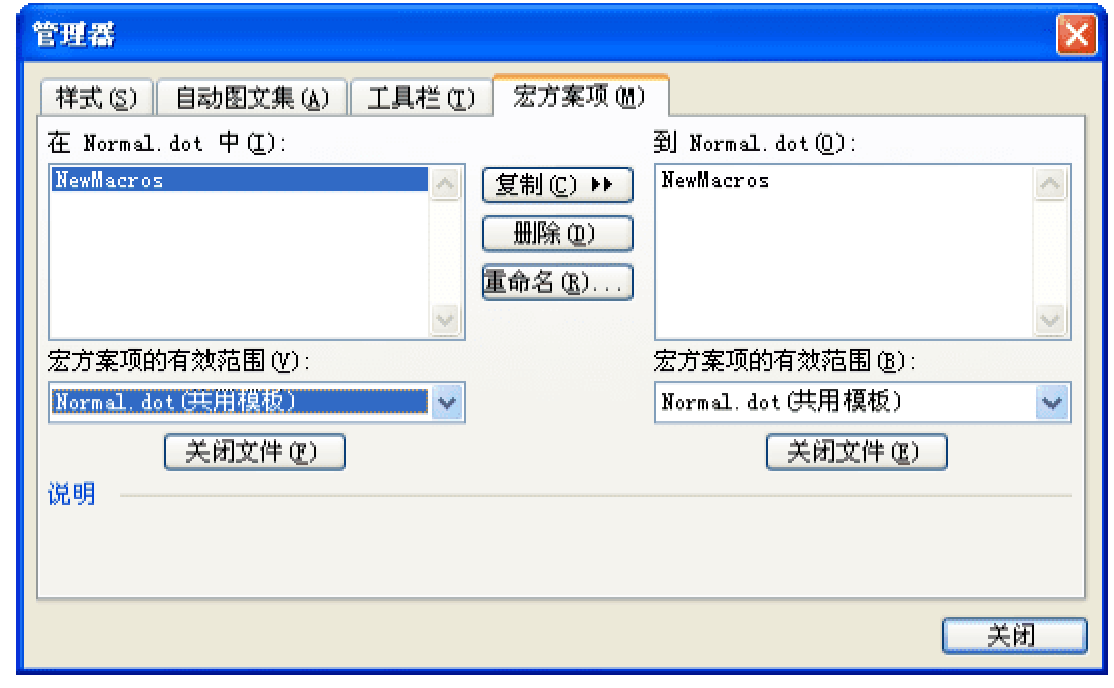


图 5.2　【管理器】对话框

退出 Word，然后先到 C 盘根目录下查看有无 autoexec.dot 文件，如果有这个文件则删除它。



找到 normal.dot 文件后删除它。Word 会自动重新生成一个干净的 normal.dot 文件。

到目录 C:\Program Files\Wicrosoft Office\Office\Startup 下查看有没有模板文件，如果有而且不是用户自己建立的，则删除它。

重新启动 Word，这时 Word 已经恢复正常了。

2) 使用专业杀毒软件

目前的杀毒软件(如瑞星等)都具备清除宏病毒的能力。当然也只能对已知的宏病毒进行检查和清除，对于新出现的病毒或病毒的变种则可能不能正常地清除，或者将会破坏文件的完整性，此时还需要手工清理。

5.2.3 蠕虫病毒

1. 蠕虫病毒的定义

蠕虫(Worm)是一种通过网络传播的恶性病毒，通过分布式网络来扩散传播特定的信息或错误，进而造成网络服务遭到拒绝并发生死锁。

蠕虫是一种广义的计算机病毒。但蠕虫又与传统的病毒有许多不同之处，如不利用文件寄生、导致网络拒绝服务、与黑客技术相结合等。在产生的破坏性上，蠕虫病毒也不是普通病毒所能比拟的，它和普通病毒的主要区别如表 5.1 所示。

表 5.1 普通病毒与蠕虫病毒的比较

病毒类型	普通病毒	蠕虫病毒
存在形式	寄生于文件	独立程序
传染机制	宿主程序运行	主动攻击
传染目标	本地文件	网络计算机

自从 1988 年美国人 Robert Morris 从实验室放出第一个蠕虫病毒以来，计算机蠕虫病毒以其快速、多样化的传播方式不断给网络世界带来灾害。特别是 1999 年以来，高危蠕虫病毒的不断出现，使世界经济蒙受了轻则几十亿，重则几百亿美元的巨大损失，如表 5.2 所示。

表 5.2 蠕虫造成的损失

病毒名称	爆发时间	造成损失
莫里斯蠕虫	1988 年	6000 多台计算机停机，经济损失达 9600 万美元
美丽杀手	1999 年	政府部门和一些大公司紧急关闭了网络服务器，经济损失超过 12 亿美元
爱虫病毒	2000 年 5 月	众多用户计算机被感染，损失超过 96 亿美元
红色代码	2001 年 7 月	网络瘫痪，直接经济损失超过 26 亿美元
求职信	2001 年 12 月	大量病毒邮件堵塞服务器，损失达数百亿美元
蠕虫王	2003 年 1 月	网络大面积瘫痪，银行自动提款机运作中断，直接经济损失超过 26 亿美元

续表

病毒名称	爆发时间	造成损失
冲击波	2003 年 7 月	大量网络瘫痪，造成数十亿美元的损失
MyDoom	2004 年 1 月	大量的垃圾邮件攻击 SCO 和微软网站，给全球经济造成了 300 多亿美元的损失

据调查，2004 年破坏性最大的十大病毒分别是网络天空(Worm.Netsky)、爱情后门(Worm.Lovgate)、SCO 炸弹(Worm.Novarg)、小邮差(Worm.Mimail)、垃圾桶(Worm.Lentin.m)、恶鹰(Worm.Bbeagle)、求职信(Worm.Klez)、高波(Worm.Agobot.3)、震荡波(Worm.Sasser)和瑞波(Backdoor.Rbot)等。从病毒名字就可以看出，几乎全部是蠕虫病毒，可见蠕虫病毒已经成为目前危害网络安全的最严重的一害。

2. 蠕虫病毒的基本结构和传播过程

(1) 蠕虫的基本程序结构包括以下 3 个模块。

① 传播模块。负责蠕虫的传播，传播模块又可以分为 3 个基本模块，即扫描模块、攻击模块和复制模块。

② 隐藏模块。侵入主机后，隐藏蠕虫程序，防止被用户发现。

③ 目的功能模块。实现对计算机的控制、监视或破坏等功能。

(2) 蠕虫程序的一般传播过程如下。

① 扫描。由蠕虫的扫描模块负责探测存在漏洞的主机。当程序向某个主机发送探测漏洞的信息并收到成功的反馈信息后，就得到一个可传播的对象。

② 攻击。攻击模块按漏洞攻击步骤自动攻击上一步骤中找到的对象，取得该主机的权限(一般为管理员权限)，获得一个 Shell。

③ 复制。复制模块通过原主机和新主机的交互将蠕虫程序复制到新主机并启动。

可见，传播模块实现的实际上是自动入侵的功能，所以蠕虫的传播技术是蠕虫技术的核心。

3. 蠕虫病毒实例——爱情后门

爱情后门(Worm.Lovgate)是一种危害性很强的蠕虫病毒，其发作时间是随机的，主要通过网络和邮件来传播，感染对象为硬盘文件夹。

当病毒运行时，将自己复制到 WINDOWS 目录下，文件名为 winrpcsrv.exe 并注册成系统服务，然后把自己分别复制到 SYSTEM 目录下，文件名为 syshelp.exe、wingate.exe，并在注册表 RUN 项中加入自身键值。病毒利用 Ntdll 提供的 API 找到 LSASS 进程，并对其植入远程后门代码(该代码将响应用户 TCP 请求建立一个远程 Shell 进程，Windows 9X 为 command.com，Windows NT/2000/XP 为 cmd.exe)，之后病毒将自身复制到 WINDOWS 目录并尝试在 win.ini 中加入 run=rpcsrv.exe，并进入传播流程。

1) 爱情后门病毒的发作过程

(1) 密码试探攻击。病毒利用 IPC 对 Guest 和 Administrator 账号进行简单密码试探，如果成功则将自己复制到对方的系统中，文件路径为 System32\stg.exe，并注册成服务，服务名为 Windows Remote Service。



(2) 放出后门程序。病毒从自身体内放出一个.dll 文件，负责建立远程 Shell 后门。

(3) 盗用密码。病毒放出一个名为 win32vxd.dll 的文件(hook 函数)用以盗取用户密码。

(4) 后门。病毒本身也将建立一个后门，等待用户联入。

(5) 局域网传播。病毒穷举网络资源，并将自己复制过去。随机地选取病毒体内的文件名，有以下几种文件，如 humor.exe、fun.exe、docs.exe、s3msong.exe、midsong.exe、billgt.exe、Card.EXE、SETUP.EXE、searchURL.exe、tamagotxi.exe、hamster.exe、news_doc.exe、PsPGame.exe、joke.exe、images.exe 和 pics,exe 等。

(6) 邮件地址搜索线程。病毒启动一个线程通过注册表 Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders 得到系统目录，并从中搜索*.ht*中的 E-mail 地址，用以进行邮件传播。

(7) 发邮件。病毒利用搜索到的 E-mail 地址进行邮件传播。邮件标题随机地从病毒体内选出：

```
Cracks!
The patch
Last Update
Test this ROM! IT ROCKS!.
Adult content!!! Use with parental advi
Check our list and mail your requests!
I think all will work fine.
Send reply if you want to be official b
Test it 30days for free.
…
```

2) 计算机中病毒的特征

(1) 计算机感染爱情后门病毒后，会出现下面的全部或部分症状。

(2) D、E、F、G 盘不能双击打开，硬盘驱动器根目录下存在 autorun.inf 文件。

(3) 在每个硬盘驱动器根目录下存在很多.zip 和.rar 压缩文件，文件名多为 pass，work，install，letter，大小约为 126KB。

(4) 在每个硬盘驱动器根目录下都存在 command.exe 文件。

(5) hxdef.exe、iexplore.exe、netmanager.exe、netmeeting.exe、winhelp.exe 等进程占用 CPU 资源。

(6) 用命令 Netstat -an 查看网络连接，会发现有很多端口处于连接或监听状态。网络速度极慢。

(7) 瑞星杀毒后出现 Windows 无法找到 command.exe 文件，要求定位该文件。

(8) 在任务管理器上看到多个 cmd.exe 进程。

3) 病毒的清除

爱情后门病毒有很多个变种，每个变种的感染方式不尽相同，所以清除病毒的最好方法是使用专业的杀毒软件，如瑞星的爱情后门专杀工具。

具体的处理过程可按以下步骤进行。

(1)　给系统账户设置足够复杂的登录密码，建议使用字母+数字+特殊字符。

(2)　关闭共享文件夹。

(3)　给系统打补丁。

(4)　升级杀毒软件病毒库，断开网络的物理连接，关闭系统还原功能后进入安全模式使用杀毒软件杀毒。

这个处理过程适用于所有病毒。一般的杀毒过程都必须经过这几步，才能保证彻底地清除病毒。

5.2.4　木马病毒

1. 木马病毒定义

木马全称为特洛伊木马(Trojan Horse，简称为 Trojan)，在计算机安全学中，特洛伊木马是指一种计算机程序，表面上或实际上有某种有用的功能，而含有隐藏的可以控制用户计算机系统、危害系统安全的功能，可能造成用户资料的泄露、破坏或整个系统的崩溃。在一定程度上，木马也可以称为计算机病毒。

2. 木马病毒工作原理

在 Windows 系统中，木马一般作为一个网络服务程序在感染了木马的计算机后台运行，监听本机一些特定端口，这个端口号多数比较大(5000 以上，但也有部分是 5000 以下的)。当该木马相应的客户端程序在此端口上请求连接时，它会与客户程序建立一个 TCP 连接，从而被客户端远程控制。

木马一般不会让人看出破绽，对于木马程序设计人员来说，要隐藏自己所设计的窗口程序，主要途径有：在任务栏中将窗口隐藏，这个只要把 Form 的 Visible 属性调整为 False，ShowInTaskBar 也设置为 False。那么程序运行时就不会出现在任务栏中了。如果要在任务管理器中隐身，只要将程序调整为系统服务程序即可。

木马是在计算机刚开机的时候运行的，进而常驻内存。其大都采用了 Windows 系统启动时自动加载应用程序的方法，包括 win.ini、system.ini 和注册表等。

在 win.ini 文件中，[WINDOWS]下面，“run=”和“load=”行是 Windows 启动时要自动加载运行的程序项目，木马可能会在这里现出原形。一般情况下，它们的等号后面什么都没有，如果发现后面跟有路径与文件名，而且不是熟悉的或以前没有见到过的启动文件项目，那么该计算机就可能中木马病毒了。当然也得看清楚，因为好多木马还通过其容易混淆的文件名来愚弄用户。例如，AOL Trojan 把自身伪装成 command.exe 文件，如果不注意可能不会发现它，而误认它为正常的系统启动文件。

在 system.ini 文件中，[BOOT]下面有 “shell=Explorer.exe”项。如果等号后面不仅仅是 explorer.exe，而是“shell=Explorer.exe 程序名”，那么后面跟着的那个程序就是木马程序，说明该计算机中了木马。

隐蔽性强的木马都在注册表中作文章，因为注册表本身就非常庞大、众多的启动项目极易掩人耳目。

HKEY-LOCAL-MACHINE\Software\Microsoft\Windows\CurrentVersion\Run



HKEY-LOCAL-MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY-LOCAL-MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx

HKEY-LOCAL-MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

HKEY-LOCAL-MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

上面这些主键下面的启动项目都可以成为木马的藏身之处。如果是 Windows NT，那还得注意 HKEY-LOCAL-MACHINE\Software\SAM 下的内容，通过 regedit 等注册表编辑工具查看 SAM 主键，里面应该是空的。

木马驻留在计算机内存以后，还要有客户端程序来控制才可以进行相应的“黑箱”操作。客户端要与木马服务器端进行通信就必须建立连接(一般为 TCP 连接)，通过相应的程序或工具都可以检测到这些非法网络连接的存在。

3. 木马病毒的检测

首先，查看 system.ini、win.ini、启动组中的启动项目。选择【开始】|【运行】命令后输入 msconfig，运行 Windows 自带的“系统配置实用程序”。

1) 查看 system.ini 文件

选中 System.ini 标签，展开[boot]目录，查看“shell=”行，正常应为“shell=Explorer.exe”，如果不是则可能中木马了。

2) 查看 win.ini 文件

选中 win.ini 标签，展开[windows]目录，查看“run=”和“load=”行，等号后面正常应该为空。

3) 查看启动组

再看启动标签中的启动项目，有没有什么非正常项目？要是有类似 netbus、netspy、bo 等关键词，极有可能是中木马了。

4) 查看注册表

选择【开始】|【运行】命令，输入 regedit，单击【确定】按钮就可以运行注册表编辑器。再展开至“HKEY-LOCAL-MACHINESoftwareMicrosoftWindowsCurrentVersionRun”目录下，查看键值中有无自己不熟悉的自动启动文件项目，比如 netbus、netspy、netserver 等的关键词。

注意，有的木马程序生成的服务器程序文件很像系统自身的文件，想由此伪装蒙混过关。比如 Acid Battery 木马，它会在注册表项“HKEY-LOCAL-MACHINESOFTWAREMicrosoft WindowsCurrentVersionRun”下加入 Explorer=“CWINDOWSexpiorer.exe”，木马服务器程序与系统自身的真正的 Explorer 之间只有一个字母的差别！

通过类似的方法对下列各个主键下面的键值进行检查：

HKEY-LOCAL-MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY-LOCAL-MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx

HKEY-LOCAL-MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

HKEY-LOCAL-MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

如果操作系统是 Windows NT，还得注意 HKEY-LOCAL-MACHINE\Software\SAM 下面的内容，如果有项目，那极有可能就是木马了。正常情况下，该主键下面是空的。

当然在注册表中还有很多地方都可以隐藏木马程序，上面这些主键是木马比较常用的隐身之处。此外，像 HKEY-CURRENT-USER\ Software\Microsoft\Windows\ CurrentVersion\Run、HKEY-USERS****\Software\Microsoft\Windows\CurrentVersion\Run 的目录下都有可能成为木马的藏身之处。最好的办法就是在 HKEY-LOCAL-MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 或其他主键下面找到木马程序的文件名，再通过其文件名对整个注册表进行全面搜索就知道它有几个藏身的地方了。

如果稍加留意，注册表各个主键下都会有个叫“(默认)”名称的注册项，而且数据显示为“(未设置键值)”，也就是空的。这是正常现象。如果发现这个默认项被替换了，那么替换它的就是木马了。

5)　其他方法

上网过程中，在进行一些计算机正常使用操作时，发现计算机速度明显起了变化、硬盘在不停地读写、鼠标不听使唤、键盘无效、自己的一些窗口在未得到自己允许的情况下被关闭、新的窗口被莫名其妙地打开等，这一切的不正常现象都可能是木马客户端在远程控制计算机的结果。

4. 木马病毒的删除

首先要将网络断开，以排除来自网络的影响，再选择相应的方法删除它。

1)　通过木马的客户端程序删除

根据前面在 win.ini、system.ini 和注册表中查找到的可疑文件名判断木马的名字和版本，比如“netbus”、“netspy”等，对应的木马就是 NETBUS 和 NETSPY。从网上找到其相应的客户端程序，下载并运行该程序，在客户端程序对应位置填入本地计算机地址 127.0.0.1 和端口号，就可以与木马程序建立连接。再由客户端的卸除木马服务器的功能来卸除木马。端口号可用“netstat -a”命令查找。

这种方法清除木马最容易，相对来说也比较彻底。但还存在一些弊端，如果木马文件名被更名，就无法通过这些特征来判断到底是什么木马了。如果木马被设置了密码，即使客户端程序可以连接上，没有密码也登录不进本地计算机。另外，如果该木马的客户端程序没有提供卸载木马的功能，那么该方法就无效了。

2)　手工删除

如果不知道中的是什么木马、无登录的密码、找不到其相应的客户端程序等，那就只能手工删除木马了。

用 msconfig 打开系统配置实用程序，对 win.ini、system.ini 和启动项目进行编辑。屏蔽掉非法启动项。如在 win.ini 文件中，将 WINDOWS 选项的“run=xxx”或“load=xxx”更改为“run=”和“load=”；编辑 system.ini 文件，将 BOOT 选项的“shell=xxx”，更改为“shell=Explorer.exe”。

用 regedit 命令打开注册表编辑器，对注册表进行编辑。先由上面的方法找到木马的程序名，再在整个注册表中搜索，并删除所有木马项目。由查找到的木马程序注册项，分析木马文件在硬盘中的位置。启动到纯 MS-DOS 状态(而不是在 Windows 环境中开个 MS-DOS 窗口)，用 del 命令将木马文件删除。如果木马文件是系统、隐藏或只读文件，还要通过“attrib -s -h -r”将对应文件的属性改变，才可以删除。



为保险起见，重新启动以后再由上面各种检测木马的方法对系统进行检查，以确保木马的确被删除了。

目前也有一些木马是将自身的程序与 Windows 的系统程序进行了绑定(也就是感染了系统文件)。比如常用到的 explorer.exe，只要 explorer.exe 一得到运行，木马也就启动了。这种木马可以感染可执行文件。由手工删除文件的方法处理木马后，一运行 explorer.exe，木马又得以复生！这时要删除木马就得连 explorer.exe 文件一起删除掉，再从其他相同操作系统版本的计算机中将该文件复制过来。

5. 木马病毒实例

Internet 上每天都有新的木马出现，所采取的隐蔽措施也是五花八门。下面介绍几种常见的木马病毒的清除方法。

1) trojan.agent 病毒的清除

清除 trojan.agent 病毒可在安全模式下进行以下处理。

(1) 重启计算机进入安全模式。

(2) 通过控制面板打开【添加删除程序】对话框，找到 windirected2.0 并卸载。

(3) 在安全模式下，打开控制面板的 Internet 选项，单击【删除文件】按钮，打开删除文件对话框，选中【删除所有脱机内容】复选框。

(4) 在安全模式下删除以下文件夹。

C:\Windows\System32\mscache

C:\Windows\System32\msicn

(5) 重启计算机到正常模式，再用杀毒程序全盘扫描。

2) Trojan.psw.agent.any 病毒的清除

Trojan.psw.agent.any 病毒会自动将用户的 IE 主页锁定为一个名叫“9505 上网导航”的网站，并会自动从网上下载新的变种病毒。该病毒运行后会将自身复制到系统文件目录中，文件名为 msprt.dll，同时将自身复制到 QQ 软件安装目录下，并从互联网上下载染毒的 riched32.dll 文件覆盖原有文件，使用户启动 QQ 时自动运行病毒。该病毒还会修改系统配置文件，使用户访问其他网站时自动跳转到“9505 上网导航”网站。

可以采取以下措施预防和清除 trojan.psw.agent.any 病毒

① 升级杀毒软件到最新版本，同时开启实时监控程序，防止病毒侵入。

② 在个人防火墙的网站访问控制黑名单中加入“www.9505.com”地址，并开启家长保护功能，阻断病毒的升级途径。

③ 如果发现 IE 浏览器的首页被莫名其妙地设置为“9505 上网导航”网站，请立即使用杀毒软件查毒。

3) trojan.dropper 病毒的清除

TROJAN.Dropper，即木马捆绑和伪装工具，可以把木马捆绑到其他文件上。

如果同时按 Ctrl+Alt+Del 组合键打开【Windows 任务管理器】，单击进程，发现以下进程：hmisvc32.exe、email.exe、oi.exe、ctsvccd.exe、adservice.exe、msmonk32.exe、gesfm32.exe，则该计算机可能已经感染了 w32.randex2、w32.spybot 脚本间谍蠕虫病毒、trojan.dropper 点滴木马等病毒。 可用以下方法解决。

① 关闭系统还原的功能(Windows Me/XP)。

② 联上网络更新病毒定义库。

③ 更新完后重新开机(按 F8 键)，并且开机到安全模式或者 VGA 模式。

④ 执行全系统的扫描，并且删除侦测到有感染病毒的所有档案。

⑤ 删除被病毒自行增加到登录文件的登录值。

4) Trojan.dl 病毒的清除

Trojan.dl 病毒是一种在 Windows 系统下的特洛伊木马病毒，一般是 PE 病毒。trojan.dl 大约有 100 种，表 5.3 列举一些常见 trojan.dl 病毒全名。

表 5.3 trojan.dl 病毒的分类及名称

序 号	病毒分类	病毒名
1	Windows 下的 PE 病毒	trojan.dl.banload.css
2	Windows 下的 PE 病毒	trojan.dl.banload.cst
3	Windows 下的 PE 病毒	trojan.dl.banload.csu
4	Windows 下的 PE 病毒	trojan.dl.banload.csv
5	Windows 下的 PE 病毒	trojan.dl.vb.bdp
6	Windows 下的 PE 病毒	trojan.dl.agent.ijn
7	Windows 下的 PE 病毒	trojan.dl.vb.bdq
8	Windows 下的 PE 病毒	trojan.dl.vb.bdr
9	Windows 下的 PE 病毒	trojan.dl.qqhelper.dus
10	Windows 下的 PE 病毒	trojan.dl.qqhelper.dut
11	Windows 下的 PE 病毒	trojan.dl.vb.bdo
12	Windows 下的 PE 病毒	trojan.dl.qoologic.de
13	Windows 下的 PE 病毒	trojan.dl.agent.ilv
14	普通文件病毒	trojan.dl.agent.ilx
15	Windows 下的 PE 病毒	trojan.dl.agent.ily
16	Windows 下的 PE 病毒	trojan.dl.banload.cvw
17	Windows 下的 PE 病毒	trojan.dl.banload.cvx
18	Windows 下的 PE 病毒	trojan.dl.banload.cvy
19	Windows 下的 PE 病毒	trojan.dl.banload.cvz
20	Windows 下的 PE 病毒	trojan.dl.banload.cwa

PEL(可移植的执行体，Portable Executable)是 Windows 下的一个 32 位的文件格式，可以在安全模式下删除，其危害和一般病毒是一样的，只不过病毒通过修改可执行文件的代码中程序入口地址，变成病毒的程序入口，导致运行时执行病毒文件。

trojan.dl.agent 病毒是一个代理木马，该木马的进程文件是 dlmain 或 dlmain.dll，是用于黑客恶意攻击计算机的跳板，或代替黑客完成其他恶意任务。

代理下载器变种 BE(trojan.dl.agent.be)木马病毒通过网络传播，病毒运行后将自己安装到系统目录，同时修改系统配置文件，实现开机自动运行。病毒会连接网页，下载其他的



病毒和木马程序。下载的病毒或木马可能会盗取用户的账号、密码等信息并发送到黑客指定的信箱中。根据这些特点应该先管理启动项，把同病毒有关的程序删除，然后用杀毒软件对计算机进行检查，找到病毒的安装路径后全部删除，再进入注册表查找同病毒有关的键值，全部删除。

如果您的操作系统是 Windows XP，可按以下步骤删除 Trojan.DL.Agent.be 病毒。

① 启动计算机按 F8 键进入安全模式，然后删除以下 3 个文件：

C:\%windows\%system32\VIPTray.exe

C:\%windows\%system32\WinDefendor.dll

C:\%windows\%system32\friendly.exe

② 修复注册表键值(修改之前请务必备份注册表)为

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

修改键值 System 为空(即将键值 System 指向的数值数据删除)。

删除注册表中与 WinDefendor.dll 相关的键值。

③ 重新启动计算机。

5.3 计算机病毒的症状

计算机病毒是一段程序代码，虽然可能隐藏得很好，但也会留下蛛丝马迹。通过对这些痕迹的观察和判别，就能够发现病毒。

根据病毒感染和发作的阶段，计算机病毒的症状可以分为 3 个阶段，计算机病毒发作前症状、病毒发作时症状和病毒发作后症状。

5.3.1 病毒发作前的症状

病毒发作前是指从计算机病毒感染计算机系统、潜伏在系统内开始，一直到激发条件满足、计算机病毒发作之前的一个阶段。在这个阶段，计算机病毒的行为主要是以潜伏和传播为主。计算机病毒会以各种手法来隐藏自己，在不被发现的同时，又自我复制，以各种手段进行传播。

计算机病毒发作前常见的症状如下。

(1) 计算机运行速度变慢。在硬件设备没有损坏或更换的情况下，本来运行速度很快的计算机，速度明显变慢，而且重启后依然很慢。这很可能是计算机病毒占用了大量的系统资源，并且自身的运行占用了大量的处理器时间，造成系统资源不足所致。

(2) 以前能正常运行的软件经常发生内存不足的错误。某个以前能够正常运行的程序，程序激活时或使用应用程序中的某个功能时报告内存不足。这很可能是由于计算机病毒驻留后占用了大量内存空间造成的。

(3) 运行正常的计算机经常死机。病毒感染了计算机系统后，将自身驻留在系统内并修改了中断处理程序等，引起系统工作不稳定，造成死机现象。

(4) 操作系统无法正常激活。关机后再激活，操作系统报告缺少必要的激活文件，或激活文件受损，系统无法激活。这很可能是计算机病毒感染系统文件后使文件结构发生了

变化，无法被操作系统加载和引导。

(5) 打印和通信发生异常。在硬件没有更改或损坏的情况下，以前工作正常的打印机，突然发现无法进行打印，或打印出来的是乱码。串口设备无法正常工作，如调制解调器不拨号等。这很可能是计算机病毒驻留内存后占用了打印端口、串行通信端口的中断服务程序，使之不能正常工作。

5.3.2 病毒发作时的症状

计算机病毒发作是指满足计算机病毒发作的条件，病毒被激活，并开始破坏行为的阶段。计算机病毒发作时的表现各不相同，这与计算机病毒编写者的心态、所采用的技术手段等密切相关。

计算机病毒发作时常见的症状如下。

(1) 出现不相干的语句。这是最常见的一种现象。

(2) 播放一段音乐。这类病毒大多属于良性病毒。

(3) 产生特定的图像。单纯地产生图像的计算机病毒大多也是良性病毒，只是在发作时破坏用户的显示界面，干扰用户的正常工作。

(4) 扰乱屏幕显示。病毒被激活时，会有多种扰乱屏幕显示的现象发生，如病毒使屏幕显示内容不断抖动等。

(5) 硬盘灯不断闪烁。硬盘灯闪烁说明有硬盘读、写操作。当对硬盘有持续、大量的操作时，硬盘灯就会不停地闪烁，如格式化或者写入很大的文件，或者对某个硬盘扇区或文件反复读取。

(6) 破坏写盘操作。病毒被激活时计算机不能写盘，或者写操作改为读操作，或者在写盘时丢失写入文件的部分内容。

(7) 速度下降。病毒激活时，病毒内部的时间延迟程序启动。在时钟中断中纳入了长时间的循环计算，迫使计算机空转，速度明显下降。

(8) 破坏键盘输入。病毒激活时，会对键盘的输入进行破坏。常见的现象有：每按一次键时，扬声器响一声；病毒将键盘封住，使用户无法从键盘输入数据等。

(9) 扬声器中发出异样的声音。病毒发作时，有时会使扬声器中发出异样的声音，如警笛声、炸弹声、扬声器鸣叫、咔咔声、嘀嗒声等。

(10) 占用或侵蚀大量内存。

(11) 发出虚假警报。

(12) 干扰内部命令的执行。病毒发作时，有时会干扰 DOS 内部命令的执行，使计算机死机或不能正常工作。

(13) 计算机突然死机或重启。

(14) 强迫用户玩游戏。有些恶作剧式的计算机病毒发作时，采用某些算法简单的游戏来中断用户的工作，强迫用户一定要玩赢了才能继续工作。

(15) 攻击 CMOS。在计算机的 CMOS 区中，存有系统的重要设置数据，如系统时钟、磁盘类型、显示器类型、内存容量、加密的机器密码等。有的病毒被激活时，能够对 CMOS 区进行写入动作，破坏其中的重要数据。

(16) 破坏文件。病毒激活时，有时会使用户打不开文件，或删除欲运行的文件；有时



会保持文件的名称不变，而用其他的程序内容替换现在正在执行的文件；有时也会更改文件名。

(17) 时钟倒转。

(18) Windows 桌面图标发生变化。

(19) 自动发送电子邮件。

(20) 鼠标自己动。

(21) 干扰打印机。病毒会修改系统数据区中有关打印机的参数，使系统对打印机的控制紊乱，出现虚假报警；病毒使打印机打印输出异常，打印时断时续；病毒将送给打印机字符进行替换，使打印的内容变形。

5.3.3　病毒发作后的症状

大多数计算机病毒都属于恶性病毒，恶性病毒发作后往往会带来巨大损失。

(1)　硬盘无法激活，数据丢失。硬盘的引导扇区被病毒破坏，无法激活计算机。有些计算机病毒修改硬盘的关键内容，使得原先保存在硬盘上的数据几乎完全丢失。

(2)　以前能正常运行的应用程序经常发生死机或者非法错误。这可能是由于计算机病毒感染应用程序后破坏了应用程序的正常功能，或者计算机病毒程序本身存在着兼容性方面的问题造成的。

(3)　系统文件丢失或被破坏。通常系统文件是不会被删除或修改的，除非对计算机操作系统进行升级。但是某些计算机病毒发作时会删除或破坏系统文件，使计算机系统无法正常激活。

(4)　文件目录发生混乱。目录发生混乱有两种情况：一种是确实将目录结构破坏，将目录扇区作为普通扇区，填入无意义的数据，且无法恢复；另一种是将真正的目录区转移到硬盘的其他扇区中，只要内存中存有该病毒，它就能够将正确的目录扇区读出，并且在应用程序需要访问该目录时提供正确的目录项，使得从表面上看来与正常情况没有两样。但是，一旦内存中没有该计算机病毒，通常的目录访问方式将无法访问到原先的目录扇区，这种破坏还是能够恢复的。

(5)　病毒破坏宿主程序。病毒对宿主程序的感染采用覆盖重写的方法。被覆盖宿主程序的源代码丢失，主程序被永久性损坏，病毒还能使宿主程序变成碎片。此类病毒是恶性病毒，宿主程序染毒后只能被删除。病毒的感染频率越高，其杀伤力越大。

(6)　部分文档丢失或被破坏。

(7)　文件内容颠倒。在使用这些文件之前，病毒预先将其内容恢复原样，而使用户觉察不到。这些文件是以被病毒颠倒后的形态存入磁盘的。一旦消除了病毒，由于无法恢复原内容，这些文件将全部报废。

(8)　部分文件自动加密码。有些计算机病毒利用加密算法，将加密密钥保存在病毒程序体内或其他隐蔽的地方，被感染的文件被加密，如果内存中驻留有这种病毒，那么在系统访问被感染的文件时它自动将文件解密，使用户察觉不到。一旦这种计算机病毒被清除，那么被加密的文档就很难恢复。

(9)　内部堆栈溢出。MS-DOS 系统内部有几个内部堆栈，不同类型的功能调用不同的内部堆栈。DOS 的不可重入，就是因为内部堆栈的值遭到破坏。有的病毒会导致 DOS 内



部堆栈溢出。

(10) 计算机重新激活时格式化硬盘。autoexec.bat 文件在每次系统重新激活时都会自动运行，病毒修改这个文件，并增加 Format C:项，导致计算机重新激活时硬盘被格式化。

(11) 禁止分配内存。病毒常驻内存后，监视程序的运行，凡是要求分配内存的程序，运行将受阻。

(12) 破坏主板。目前新型主板采用“软跳线”连接的越来越多，这正好给病毒以可乘之机。“软跳线”是指在 BIOS 中就能改动 CPU 的电压、外频和倍频。病毒可以通过修改 BIOS 参数，加高 CPU 电压使其过热而烧坏；或提高 CPU 的外频，使 CPU 和显卡、内存等外设超负荷工作而烧坏，这类事件的前兆就是死机。所以，如果发现机器经常死机，就要立即到 CMOS 中查看以上参数是否改动。值得庆幸的是，目前很多新出的主板都有 CPU 温度监测功能，一旦 CPU 超温就立即降频报警，以免烧坏硬件。

(13) 破坏光驱。光驱中的光头在读不到信号时就会加大激光发射功率，因而会降低光驱的寿命。病毒可以让光头走到盘片边缘无信号区域时不停地读盘，以加大光头发射功率，从而损坏光驱。因此要经常留意光驱灯的闪亮情况，判断光驱是否正常工作。

(14) 破坏显卡。目前很多中、高档显卡都可以手动改变其芯片的频率，且修改的方法比较简单，在 Windows 9X 注册表中即可修改。这使病毒可以利用这种方法改动显卡的“显频”，以迫使显卡超负荷工作直至烧坏。这种事件的前兆也是死机。所以，死机时不要忽视对“显频”的检查。

(15) 花屏。如果显示器在使用过程中出现了花屏，要立即关掉显示器的电源，重新启动后进入安全模式再查找原因。

(16) 浪费喷墨打印机的墨水。喷墨打印机的喷头很容易堵塞，为此打印机公司专门发明了浪费墨水的“清洗喷头”功能，即让大量墨水冲出喷头，清除杂物。于是病毒便趁此机会一次次调用该功能。预防这种病毒的唯一办法就是打印机不用时就关掉。其实只要经常注意打印机上的模式灯就可以了，清洗喷头时它通常是一闪一闪的。另外，还要仔细倾听它的声音，清洗喷头时打印头为了加热总是来回走动几下。

(17) 系统文件的时间、日期、大小发生变化。这是最明显的计算机病毒感染迹象。计算机病毒感染应用程序文件后，会将自身隐藏在原始文件的后面，文件大小会有所增加，文件的访问、修改日期和时间也会被改为感染时的时间。

(18) Word 文档打开后，该文件另存时只能以模板方式保存。这往往是打开的 Word 文档中感染了 Word 宏病毒的缘故。

(19) 磁盘空间迅速减少。这可能是由计算机病毒感染造成的。经常浏览网页、回收站中的文件过多、临时文件夹中的文件数量过多过大、计算机系统有过意外断电等情况也可能会造成可用的磁盘空间迅速减少。另一种情况是在 Windows 95/98 下内存交换文件会随着应用程序运行的时间和进程的数量增加而增长，同时，运行的应用程序数量越多，内存交换文件就越大。

(20) 网络驱动器卷或共享目录无法调用。对于有读权限的网络驱动器卷、共享目录等无法打开、浏览，或者对有写权限的网络驱动器卷、共享目录等无法创建、修改文件。虽然目前很少有纯粹针对网络驱动器卷和共享目录的计算机病毒，但计算机病毒的某些行为可能会影响对网络驱动器卷和共享目录的正常访问。



(21) 基本内存发生变化。在 DOS 下用 mem/c/p 命令查看系统中内存使用状况时，发现基本内存总字节数比正常的 640KB 要小，一般少 1～2KB。这通常是由于计算机系统感染了引导型计算机病毒所造成的。

(22) 陌生人发来的电子邮件。

(23) 自动链接到一些陌生的网站。

5.4　反病毒技术

网络反病毒技术包括预防病毒、检测病毒和杀毒等 3 种技术。

(1)　预防病毒技术。它通过自身常驻系统内存，优先获得系统的控制权，监视和判断系统中是否有病毒存在，进而阻止计算机病毒进入计算机系统和对系统进行破坏。

(2)　检测病毒技术。它是通过病毒的特征来判断病毒行为、类型等的技术。

(3)　杀毒技术。它通过对计算机病毒的分析，开发出具有删除病毒程序并恢复源文件的软件。

病毒的繁衍方式、传播方式不断地变化，反病毒技术也应该在与病毒对抗的同时不断推陈出新。“预防为主，治疗为辅”这一方针也完全适用于计算机病毒的处理。

5.4.1　预防病毒技术

防治感染病毒主要有两种手段：一种是用户遵守和加强安全操作控制措施，在思想上要重视病毒可能造成的危害；另一种是在安全操作的基础上，使用硬件和软件防病毒工具，利用网络的优势，把防病毒纳入到网络安全体系之中，形成一套完整的安全机制，使病毒无法逾越计算机安全保护的屏障，病毒便无法广泛传播。实践证明，通过这些防护措施和手段，可以有效地降低计算机系统被病毒感染的概率，保障系统的安全、稳定运行。

1. 病毒预防

对病毒的预防在病毒防治工作中起主导作用。病毒预防是一个主动的过程，不是针对某一种病毒，而是针对病毒可能入侵的系统薄弱环节加以保护和监控。而病毒治疗属于一个被动的过程，只有在发现一种病毒进行研究以后，才能找到相应的治疗方法，这也是杀毒软件总是落后于病毒软件的原因。所以，病毒的防治重点应放在预防上。

预防计算机病毒要从以下几个方面着手。

1)　检查外来文件

对从网络上下载的程序和文档应十分小心。在执行文件或打开文档之前，检查是否有病毒。使用抗病毒软件动态检测来自互联网(含 E-mail)的所有文件。电子邮件的附件必须检查病毒后再打开，并在发送邮件之前检查病毒。从外部取得的光盘及下载的文档，应检查病毒后再使用。压缩后的文件应解压缩后检查病毒。

2)　局域网预防

为减少服务器上文件感染的危险，网络管理员应使用以下一些网络安全措施。

(1)　用户访问约束，对可执行文件设置“read-only”或“execute only”权限。

(2)　使用抗病毒软件动态检查使用的文件。

(3) 用抗病毒软件经常扫描服务器，及时发现问题和解决问题。

(4) 使用无盘工作站可以降低计算机网络感染的风险。

在网络上运行一个新软件之前，断开网络，在单独的计算机上运行测试，如果确认没有病毒，再到网络上运行。

3) 购买正版软件

购买或复制正版软件，可以降低感染的风险。另外，到可信赖的站点下载资源。但如何确定一个站点是安全的，目前还没有有效的方法。

4) 小心运行可执行文件

即使该文件是从文件服务器上下载的，也不要运行没有确认的文件。使用从可靠站点下载的程序，同时用抗病毒软件进行检测。如果该文件是从 BBS 或新闻组下载的，也不要匆忙运行。等一段时间，看有没有该类文件含病毒的报道。

使用一些能够驻留内存的防病毒软件，一旦被感染的文件执行，抗病毒软件会检测到该病毒，并阻止其继续运行。

5) 使用确认和数据完整性工具

这些工具保存磁盘系统区的数据和文件信息(校验和、大小、属性、最近修改时间等)。周期性地比较这些信息，发现不一致，则可能存在病毒或者木马。经常使用 MEM、CHKDSK 及 PCTOOLS 等工具检查内存的使用情况。若基本内存少于 640KB，则有中毒的可能。

6) 周期性备份工作文件

备份源代码文件、数据库文件和文档文件等的开销远小于病毒感染后恢复它们的开销。

7) 留心计算机出现的异常

计算机异常包括操作突然中止、系统无法启动、文件消失、文件属性自动变更、程序大小和时间出现异常、非使用者意图的计算机自行操作、计算机有不明音乐传出或死机，硬盘的指示灯持续闪烁、系统的运行速度明显变慢及上网速度缓慢等。当发现硬盘资料已遭到破坏时，不必急忙格式化硬盘，因病毒不可能在短时间内将全部硬盘资料破坏，故可利用灾后重建的解毒程序加以分析，重建受损扇区。

8) 及时升级抗病毒工具的病毒特征库和有关的杀毒引擎

升级工作应形成一种制度，制定升级周期。利用安全扫描工具定时扫描系统和主机。若发现漏洞，及时寻找解决方案，从而减少被病毒和蠕虫感染的机会。

9) 建立健全网络系统安全管理制度，严格操作规程和规章制度

管理好共享的个人计算机，确认何人、何时作何使用等。在整个网络中采用抗病毒的纵深防御策略，建立病毒防火墙，在局域网和 Internet 以及用户和网络之间进行隔离。

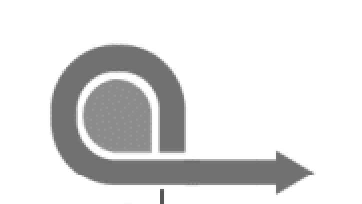
此外，还有其他的预防措施，如不需要每次从软盘启动，不要依赖于 BIOS 内置的病毒防护，不要过分相信文档编辑器内置的宏病毒保护等。

当使用一种能查能杀的抗病毒软件时，最好是先查毒，找到带毒文件后，再确定是否进行杀毒操作。因为查毒不是危险操作，它可能产生误报，但绝不会对系统造成任何损坏；而杀毒是危险操作，有可能破坏程序。

2. 网络病毒的防治

1) 基于工作站的防治方法

工作站是网络的门，只要将这扇门关好，就能有效地防止病毒的入侵。单机反病毒手



段，如单机反病毒软件、防病毒卡等同样可保护工作站的内存和硬盘，因而这些手段在网络反病毒大战中仍然大有用武之地，在一定程度上可以有效阻止病毒在网络中的传播。

由于受硬件防毒技术的影响，反病毒专家还推出了另一种基于工作站的病毒防治方法，这就是工作站病毒防护芯片。

这种方法是将防病毒功能集成在一个芯片上，安装于网络工作站，以便经常性地保护工作站及其通往服务器的途径，其基本原理是基于网络上的每个工作站都要求安装网络接口卡，而网络接口上有一个 Boot ROM 芯片，因为多数网卡的 Boot ROM 并没有充分利用，都会剩余一些使用空间，所以如果防毒程序够小，就可以安装在 Boot ROM 的剩余空间内，而不必另插一块芯片。这样，将工作站存取控制与病毒保护能力合二为一，从而免去许多烦琐的管理工作。

市场上 Chipway 防毒芯片就是采用这种网络防毒技术的。在工作站 DOS 引导过程中，ROMBIOS、Extended BIOS 装入后，Partition Tab 装入前，Chipway 将会获得控制权，这样可以防止引导型病毒入侵。

Chipway 特点如下。

(1) 不占主板插槽，避免了冲突。

(2) 遵循网络上国际标准。

(3) 具有其他工作站的防毒产品的优点。

2) 基于服务器的防治方法

服务器是网络的核心，一旦服务器被病毒感染，就会使整个网络陷于瘫痪。目前，基于服务器的防治病毒方法大都采用了以 NLM(Netware Loadable Module，可装载模块)技术进行程序设计，以服务器为基础，提供实时扫描病毒能力。

市场上较有代表性的产品如 Intel 公司的 LANdesk Virus Protect、Symantec 公司的 Center PointAnti-Virus、S&SSoftware International 公司的 Dr. Solomon's Anti-Virus Toolkit，以及我国北京威尔德计算机公司的 LANClear For Netware 等都是采用了以服务器为基础的防病毒技术。这些产品的目的都是保护服务器，使服务器不被感染。

基于网络服务器的实时扫描病毒的防护技术一般具有以下功能。

(1) 扫描范围广。采用此技术，可随时对服务器中的所有文件实施扫描，并检查其是否带毒。若有带毒文件，则向网络管理员提供几种处理方法，允许用户清除病毒，或删除带毒文件，或更改带毒文件名成为不可执行文件名，并隔离到一个特定的病毒文件目录。

(2) 实时在线扫描。网络病毒技术必须保持全天 24h 监控网络中是否有带毒文件进入服务器。为保证病毒监测的实时性，通常采用多线索的设计方法，让检测程序作为一个可以随时激活的功能模块。

(3) 服务器扫描选择。该功能允许网络管理员定期检查服务器中是否带毒，例如可按每月、每星期、每天集中扫描网络服务器。

(4) 自动报告功能及病毒存档。当带毒文件有意或无意间被复制到服务器中时，网络防病毒系统必须立即通知网络管理员，同时记入档案。病毒档案一般包括病毒类型、病毒名称、带毒文件所存的目录及工作站标识等，另外还登记对病毒的处理方法。

(5) 工作站扫描。考虑到基于服务器的防病毒软件不能保护本地工作站硬盘，有效方法是在服务器上安装防毒软件，同时在网上的工作站内存中调入常驻扫描程序，实时检测

在工作站中运行的程序，如 LANdesk Virus Protect 采用 LPScan、LANClear For Netware 采用 World 程序等。

(6)　对用户开放的病毒特征接口。若使防病毒系统能对付不断出现的新病毒，就要求开发商能够使自己的产品具有自动升级功能，其典型的做法是开放病毒特征数据库。用户随时将遇到的带毒文件，经过病毒特征分析程序，自动将病毒特征加入特征库，以随时增强抗毒能力。

基于网络服务器的防治病毒方法的优点主要表现在不占用工作站的内存，可以集中扫毒，能实现实时扫描功能，以及软件安装和升级都很方便等。特别是联网机器很多时，利用这种方法比为每台工作站都安装防病毒产品要节省成本。

病毒的入侵必将对系统资源构成威胁，即使是良性病毒也要侵吞系统的宝贵资源，因此防治病毒入侵要比病毒入侵后再加以清除重要得多。抗病毒技术必须建立“预防为主，消灭结合”的基本观念。

5.4.2　检测病毒技术

要判断一个计算机系统是否感染病毒，首先要进行病毒检测，检测到病毒的存在后才能对病毒进行消除和预防，所以病毒的检测是至关重要的。通过检测及早发现病毒，并及时进行处理，可以有效地抑制病毒的蔓延，尽可能地减少损失。

检测计算机上是否被病毒感染，通常可以分为两种方法，即手工检测和自动检测。

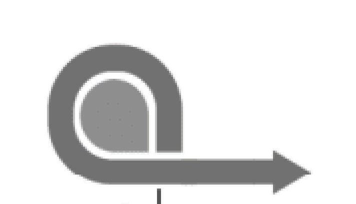
(1)　手工检测是指通过一些工具软件，如 Debug.com、Pctools.exe、Nu.com 和 Sysinfo.exe 等进行病毒的检测。其基本过程是利用这些工具软件，对易遭病毒攻击和修改的内存及磁盘的相关部分进行检测，通过与正常情况下的状态进行对比来判断是否被病毒感染。这种方法要求检测者熟悉计算机指令和操作系统，操作比较复杂，容易出错且效率较低，适合计算机专业人员使用，因而无法普及。但是，使用该方法可以检测和识别未知的病毒，以及检测一些自动检测工具不能识别的新病毒。

(2)　自动检测是指通过一些诊断软件和杀毒软件，来判断一个系统或磁盘是否有毒，如使用瑞星、金山毒霸、江民杀毒软件等。该方法可以方便地检测大量病毒，且操作简单，一般用户都可以操作。但是，自动检测工具只能识别已知的病毒，而且它的发展总是滞后于病毒的发展，所以自动检测工具总是对相对数量的病毒不能识别。

对病毒进行检测可以采用手工方法和自动方法相结合的方式。检测病毒的技术和方法主要有以下几种。

1. 比较法

比较法是将原始备份与被检测的引导扇区或被检测的文件进行比较。比较时可以利用打印的代码清单(比如 Debug 的 D 命令输出格式)进行比较，或用程序来进行比较(如 DOS 的 DISKCOMP、FC 或 PCTOOLS 等其他软件)。这种比较法不需要专门的查杀计算机病毒程序，只要用常规 DOS 软件和 PCTOOLS 等工具软件就可以进行。而且用这种比较法还可以发现那些尚不能被现有的查毒程序发现的计算机病毒。因为计算机病毒传播得很快，新的计算机病毒层出不穷，而且目前还没有研究出通用的能查出一切计算机病毒，或通过代码分析可以判定某个程序中是否含有计算机病毒的查毒程序，发现新计算机病毒就只能依



靠比较法和分析法，有时必须将二者结合起来一同使用。

使用比较法能发现异常，如文件长度改变，或虽然文件长度未发生变化，但文件内的程序代码发生了变化。对硬盘主引导扇区或对 DOS 的引导扇区做检查，比较法能发现其中的程序代码是否发生了变化。由于要进行比较，保存好原始备份是非常重要的，制作备份时必须在无计算机病毒的环境下进行，制作好的备份必须妥善保管，贴上标签，并加上写保护。

比较法的优点是简单、方便，不需要专用软件。缺点是无法确认计算机病毒的种类和名称。另外，造成被检测程序与原始备份之间差别的原因尚需进一步验证，以查明是由于计算机病毒造成的，还是由于 DOS 数据被偶然原因，如突然停电、程序失控、恶意程序等破坏的。此外，当找不到原始备份时，用比较法也不能马上得到结论。因此制作和保留原始主引导扇区和其他数据备份是至关重要的。

2. 特征代码法

特征代码法是用每一种计算机病毒体含有的特定字符串对被检测的对象进行扫描。如果在被检测对象内部发现了某一种特定字符串，就表明发现了该字符串所代表的计算机病毒，这种计算机病毒扫描软件称为 Virus Scanner。

计算机病毒扫描软件由两部分组成：一部分是计算机病毒代码库，含有经过特别选定的各种计算机病毒的代码串；另一部分是利用该代码库进行扫描的程序，目前常见的对已知计算机病毒进行检测的软件大多采用这种方法。计算机病毒扫描程序能识别的计算机病毒的数目完全取决于病毒代码库内所含病毒的种类多少。显然，库中病毒代码种类越多，扫描程序能识别的计算机病毒就越多。

计算机病毒代码串的选择是非常重要的。如果随意从计算机病毒体内选一段作为代表该计算机病毒的特征代码串，由于在不同的环境中，该特征串可能并不真正具有代表性，因而，选这种串作为计算机病毒代码库的特征串是不合适的。

另一种情况是，代码串不应含有计算机病毒的数据区，因为数据区是会经常变化的。代码串一定要在仔细分析程序之后选出最具代表特性的，足以将该计算机病毒区别于其他计算机病毒的字符串。一般情况下，代码串由连续的若干个字节组成，但是有些扫描软件采用的是可变长串，即在串中包含有一个到几个模糊字节。扫描软件遇到这种串时，只要使除模糊字节之外的字符串都能完全匹配，就能判别出计算机病毒。

除了前面提到的特征串的规则外，最重要的一条是特征串必须能将计算机病毒与正常的非计算机病毒程序区分开。如果将非计算机病毒程序当成计算机病毒报告给用户，是假警报，就会使用户放松警惕，若真的计算机病毒一来，破坏就严重了，而且，若将假警报送给防杀计算机病毒的程序，会将正常程序“杀死”。

采用病毒特征代码法的检测工具，面对不断出现的新病毒，必须不断更新版本，否则检测工具会老化，逐渐失去实用价值。病毒特征代码法无法检测新出现的病毒。

特征代码法的实现步骤如下。

(1) 采集已知病毒样本。如果病毒既感染.com 文件又感染.exe 文件，则要同时采集 COM 型病毒样本和 EXE 型病毒样本。

(2) 在病毒样本中抽取特征代码，抽取的代码必须比较特殊，不大可能与普通正常程

序代码相吻合。抽取的代码要有适当长度，一方面维持特征代码的唯一性，在保持唯一性的前提下，尽量使特征代码长度短些，以减少空间与时间开销。在既感染.com 文件又感染.exe 文件的病毒样本中，要抽取两种样本共有的代码，并将特征代码纳入病毒数据库。

(3)　打开被检测文件，在文件中搜索，检查文件中是否含有病毒数据库中的病毒特征代码。如果发现与病毒特征代码完全匹配的字串符，便可以断定被查文件感染何种病毒。

特征代码法的优点是检测准确快速、可识别病毒的名称、误报警率低，依据检测结果可做解毒处理。

特征代码法的缺点是不能检测未知病毒，且搜集已知病毒的特征代码费用开销大，在网络上效率低。

3. 分析法

分析法是防杀计算机病毒不可缺少的重要技术，任何一个性能优良的防杀计算机病毒系统的研制和开发都离不开专门人员对各种计算机病毒的详尽而准确的分析。

一般来说，使用分析法的人是防杀病毒的技术人员。使用分析法的步骤如下。

(1)　确认被观察的磁盘引导扇区和程序中是否含有计算机病毒。

(2)　确认计算机病毒的类型和种类，判定其是否是一种新的计算机病毒。

(3)　弄清计算机病毒体的大致结构，提取用于特征识别的字符串或特征字，并添加到计算机病毒代码库供计算机病毒扫描和识别程序使用。

(4)　详细分析计算机病毒代码，为制定相应的防杀计算机病毒措施制订方案。

使用分析法要求具有比较全面的有关计算机、DOS、Windows、网络等的结构和功能调用，以及与计算机病毒相关的各种知识，这是与其他检测计算机病毒方法的不同之处。

此外，还需要反汇编工具、二进制文件编辑器等用于分析的工具程序和专用的试验计算机。因为即使是很熟练的防杀计算机病毒技术人员，使用性能完善的分析软件，也不能保证在短时间内将计算机病毒代码完全分析清楚。而计算机病毒有可能在分析阶段继续传染甚至发作，把软盘、硬盘内的数据完全毁坏，这就要求分析工作必须在专门设立的试验计算机上进行。在不具备条件的情况下，不要轻易开始分析工作，很多计算机病毒采用了自加密、反跟踪等技术，使得分析计算机病毒的工作经常是冗长和枯燥的。特别是某些文件型计算机病毒的代码长度可达 10KB 以上，并与系统的层次关联，使详细的剖析工作十分复杂。

分析的步骤分为静态分析和动态分析两种。静态分析是指利用反汇编工具将计算机病毒代码打印成反汇编指令程序清单后进行分析，以便了解计算机病毒分成哪些模块，使用了哪些系统调用，采用了哪些技巧，并将计算机病毒感染文件的过程翻转为清除该计算机病毒、修复文件的过程。分析人员的素质越高，分析过程越快、理解越深。动态分析则是指利用 Debug 等调试工具在内存带毒的情况下，对计算机病毒做动态跟踪，观察计算机病毒的具体工作过程，以进一步在静态分析的基础上理解计算机病毒的工作原理。在计算机病毒编码比较简单的情况下，动态分析不是必需的。但当计算机病毒采用了较多的技术手段时，必须使用动、静相结合的分析方法完成整个分析过程。

4. 校验和法

计算正常文件的校验和，并将结果写入此文件或其他文件中保存。在文件使用过程中



或使用之前，定期检查文件的校验和与原来保存的校验和是否一致，从而可以发现文件是否被感染，这种方法称为校验和法。在 SCAN 和 CPAV 工具的后期版本中除了病毒特征代码法外，还纳入校验和法，以提高其检测能力。

利用这种方法既能发现已知病毒，也能发现未知病毒，但是，它不能识别病毒类，不能报出病毒名称。由于病毒感染并非文件内容改变的唯一原因，文件内容的改变有可能是正常程序引起的，所以校验和法经常产生误报警，而且会影响文件的运行速度。

运用校验和法查杀病毒采用以下 3 种方式。

(1) 在检测病毒工具中纳入校验和法，对被查文件计算其正常状态的校验和，将校验和值写入被查文件中或检测工具中，而后进行比较。

(2) 在应用程序中，放入校验和法自我检查功能，将文件正常状态的校验和写入文件中，每当应用程序被启动时，比较现行校验和与原校验和值，实现应用程序的自检测。

(3) 将校验和检查程序常驻内存，每当启动应用程序时，自动比较应用程序内部或其他文件中预先保存的校验和。

校验和法的优点是方法简单，能发现未知病毒，也能发现被查文件的细微变化。缺点是会误报警，不能识别病毒名称，不能对付隐蔽型病毒。

5. 行为监测法

利用病毒的特有行为特征来监测病毒的方法，称为行为监测法。病毒具有某些共同行为，而且这些行为比较特殊。在正常程序中，这些行为比较罕见。当程序运行时，监视其行为，如果发现病毒行为则立即报警。

监测病毒的行为特征如下。

(1) 占有 INT13H 所有的引导型病毒，都攻击 Boot 扇区或主引导扇区。系统启动后，当 Boot 扇区或主引导扇区获得执行权时，一般引导型病毒都会占用 INT13H 功能，并在其中放置病毒所需的代码。

(2) 修改 DOS 系统数据区的内存总量。病毒常驻内存后，为防止 DOS 系统将其覆盖，必须修改系统内存总量。

(3) 对.com、.exe 文件做写入操作。病毒要感染，必须写.com、.exe 文件。

(4) 病毒程序与宿主程序进行切换。染毒程序在运行过程中，先运行病毒，而后执行宿主程序。在两者切换时有许多特征行为。

行为监测法的优点是可发现未知病毒，能够相当准确地预报未知的多数病毒。

6. 软件仿真扫描法

该技术专门用于对付多态性计算机病毒。多态性计算机病毒在每次传染时，都将自身以不同的随机数加密于每个感染的文件中，传统的特征代码法根本无法找到这种计算机病毒。因为多态性病毒代码实施密码化，而且每次所用密钥不同，即使把染毒的病毒代码相互比较，也无法找出相同的可能作为特征的稳定代码。虽然行为监测法可以检测多态性病毒，但是在检测出病毒后，因为不能判断病毒的种类，所以难以做进一步处理。软件仿真技术则能成功地仿真 CPU 执行，在 DOS 虚拟机下伪执行计算机病毒程序，安全地将其解密，然后再进行扫描。

7. 先知扫描法

先知扫描技术是继软件仿真后的又一大技术突破。既然软件仿真可以建立一个保护模式下的 DOS 虚拟机，仿真 CPU 动作并伪执行程序以解开多态变形计算机病毒，那么与应用类似的技术也可以用于分析一般程序，检查可疑的计算机病毒代码。先知扫描技术就是将专业人员用来判断程序是否存在计算机病毒代码的方法，分析归纳成专家系统和知识库，再利用软件仿真技术伪执行新的计算机病毒，超前分析出新计算机病毒代码，用于对付以后的计算机病毒。

8. 人工智能陷阱技术和宏病毒陷阱技术

人工智能陷阱是一种监测计算机行为的常驻式扫描技术。它将所有计算机病毒所产生的行为归纳起来，一旦发现内存中的程序有任何不当的行为，系统就会有所警觉，并告知使用者。这种技术的优点是执行速度快、操作简便，且可以检测到各种计算机病毒；其缺点是程序设计难度大，且不容易考虑周全。在这千变万化的计算机病毒世界中，人工智能陷阱扫描技术是具有主动保护功能的新技术。

宏病毒陷阱技术则是结合了特征代码法和人工智能陷阱技术，根据行为模式来检测已知及未知的宏病毒。其中，配合 OLE2 技术，可将宏与文件分开，使得扫描速度加快，而且能更有效地彻底清除宏病毒。

9. 实时 I/O 扫描

实时 I/O 扫描的目的在于即时对计算机上的输入/输出数据作病毒码比对，希望能够在病毒尚未被执行之前，将病毒防御于门外。理论上，这样的实时扫描技术会影响到数据的输入/输出速度。其实不然，在文件输入之后，就等于扫过一次毒了。如果扫描速度能够提高很多，这种方法确实能对数据起到一个很好的保护作用。

10. 网络病毒检测技术

随着 Internet 在全世界的广泛普及，网络已成为病毒传播的新途径，网络病毒也成为黑客对用户或系统进行攻击的有效工具，所以有效地检测网络病毒已经成为病毒检测的最重要部分。

网络监测法是一种检查、发现网络病毒的方法。根据网络病毒主要通过网络传播的特点，感染网络病毒的计算机一般会发送大量的数据包，产生突发的网络流量，有的还开放固定的 TCP/IP 端口。用户可以通过流量监视、端口扫描和网络监听来发现病毒，这种方法对查找局域网内感染网络病毒的计算机比较有效。

1) ActiveX 和 Java 病毒

大量网页中含有 ActiveX 控件和 Java 小程序(Applet)，它们在给网页带来动画和立体感效果的同时，也使上网的企业和个人用户面临新的不安全因素。

由于内存和带宽的限制，用户下载网页中的 ActiveX 控件和 Java 小程序可通过对本地硬盘的访问来获得大量本地程序的控制权限，以节约内存和带宽。恶意代码开发者正是利用这个漏洞，制造出恶意的 ActiveX 控件和 Java 程序嵌入在 Web 主页，当用户浏览这些主页时，病毒便驻留到用户的计算机中，进行偷窥、删除或毁坏文件，以及其他一些恶意活动。



在上面提到的两种新的病毒携带者中，ActiveX 更具危害性，尤其是它的早期版本OLE(对象链接和嵌入)。ActiveX 能直接调用任何 Windows 系统函数，ActiveX 组件是指一些可执行的代码如.exe 和.dll 文件等。ActiveX 主要运行在 IE 上，但在 Netscape 上通过插件也能运行 ActiveX。

Java 小程序通常存放在服务器端，由浏览器下载到用户主机，Java 小程序的代码通过Java 虚拟机在用户主机上运行。由于 Java 虚拟机运行的跨平台特点，Java 小程序在用户主机上能获得对各种操作系统函数的访问，导致病毒在各类操作系统中传播。Java 小程序可以被附加到 Web 主页或电子邮件中，一旦主页或邮件被阅读，将自动激活 Java 小程序。java.strangbrews 是第一个 Java 小程序病毒，当它获取主机控制权后，以本地程序的身份执行，感染其他 class 文件。现在，各种浏览器(如微软的 IE 和 Netscape 的 Navigator 等)都支持 ActiveX 和 Java，这为病毒的传播提供了新的手段。

JavaScript 是 Netscape 公司继 Sun 的 Java 小程序之后推出的一种脚本语言。它不仅支持 Java 小程序，同时向 Web 作者提供一种嵌入 HTML 文档进行编程的、基于对象的脚本程序设计语言，采用的许多结构与 Java 小程序相似。由于 JavaScript 可以从用户的浏览器获取对主机资源的使用权限，所以 JavaScript 也是病毒传播的重要手段。

2) 邮件病毒

邮件病毒的传播方式是通过邮件中的附件进行的。这时附件是一个带毒文件，如 Word宏病毒。病毒的制造者通常以极具诱惑力的标题，使邮件接收者点击携带病毒的邮件附件。如“爱虫”病毒以“I love you”作为邮件标题，以情书的形式诱骗收件者。

3) 基于 Web 的防病毒技术

对于网络病毒，如 ActiveX 和 Java 小程序，最简单的防护措施是在浏览器中禁止这些插件，但这直接影响了可为用户提供的服务质量。而最有效的方法是在病毒尚未被浏览器获取前，在 TCP/IP 或应用层对接收的信息进行扫描，这就是病毒防火墙或病毒网关。

传统的病毒扫描器一般包含以下组件，即病毒搜索引擎、病毒特征库和配置管理界面。

搜索引擎的设计是提高病毒扫描速度的关键技术。为提高性能，病毒扫描引擎通常利用规则和模式识别技术来对成千上万种已知的和未知的计算机病毒进行监测，这种技术能极大地提高效率，节省系统资源。

病毒防火墙除了含有传统病毒扫描器中的组件外，还增加了一些新的组件，而且各组件通过一种柔性的、面向对象的设计原则有机集成在一起。

4) 解压缩和解码

传统的病毒搜索引擎一般是在数据传输的末端对病毒进行扫描和处理，因而不需要强大的解压缩和解密功能。病毒防火墙的病毒搜索引擎也能在数据传输中捕获病毒，因为其中嵌入了强大的实时解压缩和解密模块，它们能理解文件格式，在文件从服务器传输到 PC的过程中，“阅读”文件头部，以判断哪些压缩或加密过的文件可能含有病毒，然后只对可能含有病毒的文件进行解压缩或解密。这项新的技术并没有给系统资源增添负担，因而极大地提高了病毒扫描的效率。

5) ActiveX 和 Java 扫描

病毒防火墙的 ActiveX 和 Java 病毒扫描模块中，通常从以下 3 个方面实现对 Web 信息中的恶意代码进行检测。

(1) 支持“代码认证签名”。病毒扫描器通过将 Java 小程序和 ActiveX 对象与“代码认证签名库”进行匹配，以判断 Java 小程序和 ActiveX 对象是否来自于在传输过程中未被篡改的可信源。

(2) 识别 Java 类和 COM 指令。病毒扫描器能扫描 Java 类和 COM 指令，通过将这些指令与已知的“恶意小程序模式库”匹配来判断哪些 Java 类和 COM 指令是有恶意的。

(3) 基于规则的扫描技术。这种新技术使病毒扫描器能创造一种模拟环境来分析 Java 小程序和 ActiveX 对象的行为。扫描器中的代理把自己“寄生”在 Java 小程序上，并实时监测小程序的行为，如果发现有恶意行为，代理根据系统管理员预先配置的指令停止恶意代码的执行，并向服务器报警。

6) 病毒库自动升级

在病毒防范管理中，系统管理员遇到的两个最主要的问题是客户端软件的升级和病毒感染源的跟踪。在新一代的扫描引擎中，一些防病毒生产商嵌入了具有自我管理功能的通信组件，它知道何时并怎样下载新的病毒代码文件和扫描引擎，并在没有管理员干涉的情况下为用户进行所有的配置和分发工作。

这种通信模块具有目录意识，它能嵌入到公司的目录服务中去，并向主机发送病毒通知和采取响应。例如，在某一财务部门发现了一种病毒，具有目录意识的通信模块追查出该病毒来自于远方办公地点的一封 E-mail 中的电子表格附件，它将智能化地通知远方办公地点的管理员、邮件的发送者和接收者。

7) 防邮件病毒技术

传统的防邮件病毒产品运行于客户端，它有两个主要缺点：一是只能查杀本地硬盘上的受病毒感染的文件，而真正的病毒源(位于邮件服务器上)并没有得到及时处理，如果服务器没有受到保护，可能会使整个企业内部的网络受到病毒的攻击；二是安装在 PC 上的防病毒软件需要不断升级，这必然浪费大量的时间和资源。

邮件病毒的搜索引擎软件可以安装在专用的病毒防火墙或 SMTP 邮件服务器上。为实现实时检测，防火墙必须在端口 25 实时监测流经防火墙的 SMTP 数据流，即接收所有的 SMTP 报文，检测这些邮件是否有病毒，并将这些邮件转发到邮件的目的服务器。

与 Web 病毒防火墙类似，邮件病毒防火墙必须支持压缩文件和各类编码文件的病毒扫描，因为黑客经常把病毒放入具有压缩或加密性质的附件中以躲过防病毒软件的监测。

通过网络进行传播是网络病毒的特点，病毒主要通过 HTTP、FTP 和 SMTP 协议传播到用户的主机。服务器、网络接入端和网站是病毒进入用户主机的必经之路，如果在服务器、网络接入端和网站设置病毒防火墙，可以起到大规模防止病毒扩散的目的，比单机防病毒的效果更好。

5.4.3 杀毒技术

将染毒文件的病毒代码摘除，使之恢复为可正常运行的文件，称为病毒的清除，有时也称为对象恢复。清除病毒所采用的技术称为杀毒技术。

大多数情况下，采用抗病毒软件恢复受感染的文件或磁盘。但是，如果抗病毒软件不了解该病毒，就需要把感染文件传给抗病毒软件供应商，过一段时间后才会收到解决方案。

依据病毒的种类及其破坏行为的不同，染毒后，有的病毒可以消除，有的病毒不能



消除。

1. 引导型病毒的清除

1) 引导型病毒感染时的攻击部位

① 硬盘主引导扇区。

② 硬盘或软盘的 Boot 扇区。

为保存原主引导扇区、Boot 扇区，病毒可能随意地将其写入其他扇区，从而毁坏这些扇区。

引导扇区的恢复，大多数情况下是使用 DOS SYS 命令或者 FDISK/MBR。引导扇区的恢复必须保证病毒不在 RAM 区。如果病毒的副本在 RAM 区，则该病毒会重新感染已恢复的磁盘或者硬盘。

使用 FDISK/MBR 恢复引导扇区时该命令会重写系统加载程序，但不会改变磁盘分区表，FDISK/MBR 可以清除大多数引导型病毒。然而，如果该病毒加密磁盘分区表或使用非标准的感染方法，则 FDISK/MBR 会完全丢失磁盘信息。因此，使用 FDISK/MBR 之前，一定要确认磁盘分区表没有被修改过。通过没有感染的磁盘启动到 DOS 环境，使用磁盘工具(如 Norton Disk Editor)检查该分区表是否完整。

如果不能用 SYS/FDISK 恢复引导扇区，则必须分析该病毒的执行算法，寻找到原始引导扇区的位置，并将它们移到正确位置上。

2) 修复带毒的硬盘主引导扇区

【例 5.2】 介绍清除引导型病毒的步骤。

① 用无毒软盘启动系统。

② 寻找一台同类型、硬盘分区相同的无毒计算机，将其硬盘主引导扇区写入一张软盘中。

③ 将此软盘插入染毒计算机，将其中采集的主引导扇区数据写入染毒硬盘，即可修复。

④ 硬盘、软盘 Boot 扇区染毒也可以修复。寻找与染毒盘相同版本的无毒系统软盘，执行 SYS 命令，即可修复。

引导型病毒如果将原主引导扇区或 Boot 扇区覆盖写入根目录区，被覆盖的根目录区会遭到永久性损坏。引导型病毒如果将原主引导扇区或 Boot 扇区覆盖式写入第一 FAT 表时，可以修复，方法是将第二 FAT 表复制到第一 FAT 表中。

2. 宏病毒的清除

为了恢复宏病毒，须用非文档格式保存足够的信息。RTF(Rich Text Format)适合保留原始文档的足够信息而不包含宏。然后退出文档编辑器，删除已感染的文档文件以及 normal.dot 和 start-up 目录下的文件。

经过上述操作，用户的文档信息都可以保留在 RTF 文件中。这种方式的缺点是打开和保存文档时存在格式转换，这种转换增加了处理时间。另外，正常的宏命令也不能使用。因此，在清除宏病毒之前应保存好正常的宏命令，宏病毒清除后再恢复这些宏命令。



3. 文件型病毒的清除

一般文件型病毒的染毒文件可以修复。在绝大多数情况下，感染文件的恢复都是很复杂的。如果没有必要的知识，如可执行文件格式、汇编语言等，是不可能手工清除的。

当恢复受感染的文件时，需考虑下列因素。

① 不管文件的属性(只读/系统/隐藏)，测试和恢复所有目录下的可执行文件。

② 希望确保文件的属性和最近修改时间不改变。

③ 一定考虑一个文件多重感染情况。

COM/EXE 型文件交叉感染了多个病毒，病毒代码在宿主文件头部和尾部都有时，必须正确判断出这几个病毒感染文件的先后顺序才可能修复；否则，染毒程序无法恢复。

4. 病毒的去激活

清除内存中的病毒是指把 RAM 中的病毒进入非激活状态，跟文件恢复一样，需要操作系统和汇编语言知识。

清除内存中的病毒，需要检测病毒的执行过程，然后改变其执行方式，使病毒失去传染能力。这需要全面分析病毒代码，因为不同的病毒其感染方式不同。

在大多数情况下，除去内存中的病毒必须截断病毒截获的中断，文件型病毒截获 INT 21H，引导型病毒截获 INT 13H。当然病毒可以截获其他中断，或者截获许多中断。

有的病毒对其代码有保护机制，如 YanKee 使用纠错码恢复自己。此时，病毒的恢复机制首先需要解除，因为有的病毒计算它们的 CRC 值，并把该值与原来的值比较，如果不同，则系统被重新启动，或删除磁盘扇区。因此，这种 CRC 的计算例程必须被解除。

5. 使用杀病毒软件清除病毒

计算机一旦感染了病毒，一般的用户首先想到的就是使用杀毒软件来清除病毒。杀毒软件能清除大多数病毒，而且使用方便，技术要求不高，不需要具备太多的计算机知识。但有时也会删除带毒文件，使系统不能正常运行。

使用防杀病毒软件清除计算机病毒是普通用户的首选，但需要经常升级病毒代码库，以便能清除各种新出现的病毒。

6. 网络病毒的清除

【例 5.3】 网络病毒的清除步骤。

一旦在网络上发现病毒，应立即设法清除，其操作步骤如下。

(1) 立即使用 broadcast 命令，通知所有用户退网，关闭文件服务器。

(2) 用带有写保护的、干净的系统盘启动系统管理员工作站，并立即清除本机病毒。

(3) 用带有写保护的、干净的系统盘启动文件服务器。在系统管理员登录后，使用 disable login 命令禁止其他用户登录。

(4) 将文件服务器硬盘中的重要资料备份到干净的软盘上。但千万不可执行硬盘上的程序，也千万不要在硬盘中复制文件，以免破坏被病毒搞乱的硬盘数据结构。

(5) 用杀毒软件(最好是网络杀毒软件)扫描服务器上所有卷的文件，恢复或删除被病毒感染的文件，重新安装被删除的文件。



(6) 用杀毒软件扫描并清除所有可能染上病毒的软盘或备份文件中的病毒。

(7) 用杀毒软件扫描并清除所有的有盘工作站硬盘上的病毒。

(8) 在确信病毒已经彻底清除后，重新启动网络和工作站。如有异常现象，应请网络安全与病毒防治专家来处理。

5.5 计算机病毒发展的新技术

计算机病毒的广泛传播，推动了反病毒技术的发展。新的反病毒技术的出现，又迫使计算机病毒技术再次更新。两者相互激励，呈螺旋式上升，不断地提高各自的水平，在此过程中出现了许多计算机病毒新技术，其主要目的是为了使计算机病毒能够广泛地进行传播。

5.5.1 抗分析病毒技术

抗分析病毒技术是针对病毒分析技术的，为了使病毒分析者难以清楚地分析出病毒原理，这种病毒综合采用了以下两种技术：

(1) 加密技术。这是一种防止静态分析的技术，它使分析者无法在不执行病毒的情况下阅读加密过的病毒程序。

(2) 反跟踪技术。此技术使分析者无法动态跟踪病毒程序的运行。

在无法静态分析和动态跟踪的情况下，病毒分析者是无法知道病毒工作原理的。

5.5.2 隐蔽性病毒技术

计算机病毒不需要采取隐蔽技术就能达到广泛传播的目的。计算机病毒刚开始出现时，人们对这种新生事物认识不足，然而，当人们越来越了解计算机病毒，并有了一套成熟的检测病毒的方法时，病毒若广泛传播，就必须能够躲避现有的病毒检测技术。

难以被人发现是病毒的重要特性。隐蔽好，不易被发现，可以争取较长的存活期，造成大面积的感染，从而造成大面积的伤害。隐蔽自己不被发现的病毒技术称为隐蔽性病毒技术，它是与计算机病毒检测技术相对应的，此类病毒使自己融入运行环境中，隐蔽行踪，使病毒检测工具难以发现自己。一般来说，有什么样的病毒检测技术，就有相应的隐蔽性病毒技术。

若计算机病毒采用特殊的隐形技术，则在病毒进入内存后，用户几乎感觉不到它的存在。

5.5.3 多态性病毒技术

多态性病毒是指采用特殊加密技术编写的病毒，这种病毒每感染一个对象，就采用随机方法对病毒主体进行加密，不断改变其自身代码，这样放入宿主程序中的代码互不相同，不断变化，同一种病毒就具有了多种形态。

多态性病毒是针对查毒软件而设计的，所以随着这类病毒的增多，查毒软件的编写也变得更困难，并且还会带来误报。国际上造成全球范围内的传播和破坏的第一例多态性病毒是 TEQUTLA 病毒，从该病毒的出现到编制出能够完全查出该病毒的软件，研究人员花

费了 9 个月的时间。

多态性病毒的出现给传统的特征代码检测法带来了巨大的冲击，所有采用特征代码法的检测工具和清除病毒工具都不能识别它们。被多态性病毒感染的文件中附带着病毒代码，每次感染都使用随机生成的算法将病毒代码密码化。由于其组合的状态多得不计其数，所以不可能从该类病毒中抽出可作为依据的特征代码。

多态性病毒也存在一些无法弥补的缺陷，所以，反病毒技术不能停留在先等待被病毒感染，然后用查毒软件扫描病毒，最后再杀掉病毒这样被动的状态。而应该采取主动防御的措施，采用病毒行为跟踪的方法，在病毒要进行传染、破坏时发出警报，并及时阻止病毒作出任何有害操作。

5.5.4　超级病毒技术

超级病毒技术是一种很先进的病毒技术。其主要目的是对抗计算机病毒的预防技术。

信息共享使病毒与正常程序有了汇合点。病毒借助于信息共享能够获得感染正常程序、实施破坏的机会。如果没有信息共享，正常程序与病毒相互完全隔绝，没有任何接触机会，病毒便无法攻击正常程序。反病毒工具与病毒之间的关系也是如此。如果病毒作者能找到一种方法，当一个计算机病毒进行感染、破坏时，让反病毒工具无法接触到病毒，消除两者交互的机会，那么反病毒工具便失去了捕获病毒的机会，从而使病毒的感染、破坏过程得以顺利完成。

由于计算机病毒的感染、破坏必然伴随着磁盘的读、写操作，所以预防计算机病毒的关键在于，病毒预防工具能否获得运行的机会以对这些读写操作进行判断分析。超级病毒技术就是在计算机病毒进行感染、破坏时，使得病毒预防工具无法获得运行机会的病毒技术。

一般病毒攻击计算机时，往往窃取某些中断功能，要借助 DOS 才能完成操作。例如，在 PC 中病毒要写盘，必须借助原 DOS 的 INT 13H。反病毒工具都是在 DOS 中设置了许多陷阱，监视着系统中许多病毒欲攻击的敏感点，等待病毒触碰这些警戒点，一旦掉入陷阱，病毒便被捕获。超级病毒的作者以更高的技术编写了完全不借助于 DOS 系统而能攻击计算机的病毒，此类病毒攻击计算机时，完全依靠病毒内部代码来进行操作，避免碰触 DOS 系统，因而不会掉入反病毒陷阱，使抗病毒工具极难捕获它。一般的软件或反病毒工具遇到此类病毒都失效。

超级计算机病毒目前还比较少，因为它的技术还不为许多人所知，而且编制起来也相当困难。然而一旦这种技术被越来越多的人掌握，同时结合多态性病毒技术、插入性病毒技术，这类病毒将给反病毒的艰巨事业增加困难。

5.5.5　插入性病毒技术

病毒感染文件时，一般将病毒代码放在文件头部，或者放在尾部，虽然可能对宿主代码做某些改变，但总的来说，病毒与宿主程序有明确界限。

插入性病毒在不了解宿主程序的功能及结构的情况下，能够将宿主程序拦腰截断。在宿主程序中插入病毒程序，此类病毒的编写也是相当困难的。如果对宿主程序的切断处理



不当，则很容易死机。

5.5.6 破坏性感染病毒技术

破坏性感染病毒技术是针对计算机病毒消除技术而设计的。

计算机病毒消除技术是将被感染程序中的病毒代码摘除，使之变为无毒的程序。一般病毒感染文件时，不伤害宿主程序代码。有的病毒虽然会移动或变动部分宿主代码，但在内存运行时，还是要恢复其原样，以保证宿主程序正常运行。

破坏性感染病毒则将病毒代码覆盖式写入宿主文件，染毒后的宿主文件丢失了与病毒代码等长的源代码。如果宿主文件长度小于病毒代码长度，则宿主文件全部丢失，文件中的代码全部是病毒代码。一旦文件被破坏性感染病毒感染便如同得了绝症，被感染的文件，其宿主文件少则丢失几十字节，多则丢失几万字节，严重的甚至会全部丢失。如果宿主程序没有副本，感染后任何人、任何工具都无法补救，所以此种病毒无法做常规的杀毒处理。

一般的杀毒操作都不能消除此类病毒，它是杀毒工具不可逾越的障碍。破坏性病毒虽然恶毒，却很容易被发现，因为人们一旦发现一个程序不能完成它应有的功能，一般会将其删除，这样病毒根本无法向外传播，因而不会造成太大的危害。

5.5.7 病毒自动生产技术

病毒自动生产技术是针对病毒的人工分析技术而设计的。

国外曾出现过一种叫作“计算机病毒生成器”的软件工具，该工具界面良好，并有详尽的联机帮助，易学易用，即使对计算机病毒一无所知的用户，也能随心所欲地组合出算法不同、功能各异的计算机病毒。另外，还有一种叫作“多态性发生器”的软件工具，利用此工具，可将普通病毒编译后，输出很难处理的多态性病毒。由此可见，病毒的制作已进入自动化生产的阶段。

MutationEngine 是一种程序变形器，可以使程序代码本身发生变化，而保持原有功能。利用计算得到的密钥，程序变形器产生的程序代码可以多种多样。当计算机病毒采用了这种技术时，会变成一种具有自我变异功能的计算机病毒。这种病毒程序可以衍变出各种各样变种的计算机病毒，且这种变化是由程序自身的机制生成的。单从程序设计的角度讲，这是一项很有意义的新技术，使计算机软件变成了一种具有某种“生命”形式的“活”的东西。但从保卫计算机系统安全的反病毒技术人员角度来看，这种变形病毒是不容易对付的敌手。从广义上讲，病毒自动生产技术是针对病毒的分析技术的，它不是从“质”上而是从“量”上企图压垮病毒分析者。

5.5.8 Internet 病毒技术

随着 Internet 的迅速发展，将文件附加在电子邮件中的能力在不断地提高，因而病毒的扩散速度也急剧上升，受感染的范围越来越广，而且感染方式也从软盘介质感染转到了从网络服务器到 Internet 的感染。

电子邮件在服务信息社会的同时，也为计算机病毒找到了一条新的传播途径和载体。病毒为增加隐蔽性，通常夹在电子邮件中，并附以熟悉的姓名、重要的提示或美丽的图案，

使用户不会产生任何怀疑，以诱骗用户打开邮件及其附件。

综上所述，病毒技术是多种多样的，各个方面都对反病毒技术带来严重的挑战。计算机病毒不仅仅是数量上的增长，而且在理论上和实践的技术上均有较大的发展和突破。从目前来看，计算机病毒技术领先于反病毒技术。只有详细了解病毒原理以及病毒采用的各种技术，才能更好地防治病毒。也只有对病毒技术从理论、技术上做一些超前的研究，才能对新型病毒的出现做到心中有数，达到防患于未然的目的。

5.6 防杀网络病毒的软件

5.6.1 防毒软件

防病毒软件可以检测外来的程序、文件或邮件附件，并给出实时警告或删除病毒。不同的防毒软件的保护机制各不相同，在安装时往往被设定为默认模式。在使用过程中，如果仅仅保留默认设置，或者为了提升系统性能减少了一部分保护功能，则系统很可能在某些关键时刻丧失保护。所以针对不同的防毒软件的不同设计思路要进行不同的设置，以更好地保护系统安全。

5.6.2 反病毒软件

随着计算机技术及反毒技术的发展，早期的防病毒卡也像其他计算机硬件卡(如汉字卡等)一样，逐步衰落退出市场，与此对应的，各种反病毒软件开始日益风行起来，并且经过十几年的发展，逐步经历了好几代反病毒技术的发展。

第一代反病毒技术采取单纯的病毒特征代码分析，将病毒从带毒文件中清除掉。这种方式可以准确地清除病毒，可靠性很高。后来病毒技术发展了，特别是加密和变形技术的运用，使得这种简单的静态扫描方式失去了作用。随之而来的反病毒技术也发展了一步。

第二代反病毒技术采用静态广谱特征扫描方法检测病毒，这种方式可以更多地检测出变形病毒，但另一方面误报率也有所提高，尤其是用这种不严格的特征判定方式去清除病毒带来的风险性很大，容易造成文件和数据的破坏。所以说静态防病毒技术也有难以克服的缺陷。

第三代反病毒技术的主要特点是将静态扫描技术和动态仿真跟踪技术结合起来，将查找病毒和清除病毒合二为一，形成一个整体解决方案，能够全面实现防、查、杀等反病毒所必备的各种手段，以驻留内存方式防止病毒的入侵，凡是检测到的病毒都能清除，不会破坏文件和数据。随着病毒数量的增加和新型病毒技术的发展，静态扫描技术将会使反毒软件速度降低，驻留内存防毒模块容易产生误报。

第四代反病毒技术则针对计算机病毒的命名规则，基于多位 CRC 校验和扫描机理，启发式智能代码分析模块、动态数据还原模块(能查出隐蔽性极强的压缩加密文件中的病毒)、内存解毒模块、自身免疫模块等先进的防毒技术，较好地解决了以前防毒技术顾此失彼、此消彼长的状态。

反病毒软件伴随着反病毒技术的不断提高而功能越来越强，可以清除大多数病毒。

杀毒软件市场潜力巨大，世界杀毒软件巨头之一的赛门铁克(Symantec)公司 2004 年的



收入已经达到 18.7 亿美元，其产品包括了网络安全的各个方面，杀毒产品为诺顿(Norton Antivirus)。国内的杀毒软件市场基本形成瑞星、江民、金山三足鼎立的局面。

5.6.3 瑞星杀毒软件

瑞星(http://www.rising.com.cn)是北京瑞星科技股份有限公司的产品，在国内市场占有率为 60%左右。

北京瑞星科技股份有限公司成立于 1998 年 4 月，公司以研究、开发、生产及销售计算机反病毒产品、网络安全产品和“黑客”防治产品为主，软件产品全部拥有自主知识产权，能够为个人、企业和政府机构提供全面的信息安全解决方案。

5.6.4 金山毒霸

金山毒霸(http://db.kingsoft.com)是金山软件股份有限公司的产品，在国内市场占有率为 15%左右。

金山软件创建于 1988 年，金山毒霸是中国信息安全及反病毒领域极具品牌影响力、拥有较高市场占有率和领先技术的产品。

5.6.5 江民杀毒软件

江民(http://www.jiangmin.com)杀毒软件 KV2006 是江民科技公司的最新产品，在国内市场占有率为 15%左右。

江民科技公司成立于 1996 年，研发和经营范围涉及：单机、网络反病毒软件；单机、网络黑客防火墙；邮件服务器防病毒软件等一系列信息安全产品。

5.7 病毒与漏洞的关系

网络安全设备厂商常常会有这样的苦恼，比如 IPS 时常检测到大量来自内网的攻击，而用户对这种攻击不了解，希望厂商为其清理攻击源。但这种情况往往是因为用户网络中有节点感染了带蠕虫特征的病毒，这些病毒的清除工作比较繁琐。下面讨论漏洞与病毒的关系，解开病毒发起攻击的相关疑惑。

5.7.1 漏洞与病毒的概念

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未经授权的情况下访问或破坏系统。漏洞会影响到很大范围的软、硬件设备，包括操作系统及其上的应用软件、网络客户端和服务器，甚至路由器和安全防火墙等。漏洞问题是与时间紧密相关的。随着时间的推移及用户使用的深入，系统中存在的漏洞会不断暴露出来，这些漏洞也会不断被系统供应商发布的补丁软件修补，IPS 设备也会做相应防护，但是潜在的漏洞不会因为这些措施而消失，依然存在并可能在某个时间点被发现，个别漏洞隐藏的时间可长达十数年之久。

计算机病毒是指编制者在计算机程序中插入的破坏计算机功能或者破坏数据、影响计

算机使用并且能够自我复制的一组计算机指令或者程序代码。计算机病毒可以像生物病毒一样进行繁殖，当正常程序运行的时候，它也进行自身复制，有无繁殖、感染的特征是判断某段程序是否为计算机病毒的首要条件。计算机病毒可通过各种可能的渠道，如可移动存储介质、计算机网络去感染其他计算机。当在一台机器上发现病毒时，往往曾在这台计算机上用过的 U 盘已感染上了病毒，而与这台机器相联网的其他计算机可能也被该病毒感染上了。

5.7.2 漏洞辅助病毒传播

病毒的传播途径多种多样，基于社会工程学的电子邮件、网页及 P2P 文件共享较为常见。比较直接的方式是，病毒传播者将病毒放在电子邮件中寄给受害者，引诱受害者打开电子邮件中的带病毒.exe 文件而感染病毒，或者通过 P2P 共享或网页链接的方式，欺骗受害者打开病毒文件。对于安全意识较好的用户，这些伎俩均难以得逞。但是如果病毒具有可通过漏洞进行传播的能力，而用户系统没有针对病毒攻击的目标漏洞采取防护措施，用户系统将可能在不做任何操作的情况下被病毒感染。常见的病毒利用漏洞传播的方式有如下几种。

1. 利用网站漏洞进行网页挂马

通过对网站漏洞的利用，黑客可以将病毒植入到访问量比较大的网站，用户一旦访问这些网站即被病毒感染。很多比较大的门户网站也发生过被挂马的事件。这种方式利用了网站的影响力及用户对常用网站基于信任的权限设置，大大增加了病毒感染数量。病毒传播者要利用网站漏洞进行网页挂马传播病毒，必须要获取对站点文件的修改权限，而获取该站点的 WebShell(网站的后门工具，对服务器有某种程度的操作权限)是最普遍的做法。可供病毒传播者实施的攻击手段比较多，比如注入漏洞、跨站漏洞、旁注漏洞、上传漏洞和系统漏洞都可被利用。对于这种病毒传播方式，主要靠网站通过及时修补漏洞、部署 IPS 等来防御，网站用户安装杀毒软件和即时更新浏览器相关补丁也是必不可少的措施。

2. 利用应用程序漏洞传播病毒

很多常用的办公软件，如微软 Office 家族及 Adobe 的 Acrobat/Reader 系列，由于其功能强大、实现复杂，基本每月均会报出新的漏洞，而这些漏洞均有可能被病毒传播者利用。网页浏览中最常用的 Flash 播放器插件 Adobe Flash Player，也是曾经的漏洞大户，理所当然地成为病毒传播者比较重视的传播途径。事实上，国内许多口碑不错的应用软件，也已经成为病毒传播者的目标。越来越多的黑客，已经把目光从系统漏洞转向第三方应用程序漏洞去达到不法目的，主要原因是应用软件厂商的安全响应速度不及系统软件厂商快，并且应用软件用户群的安全意识和安全知识普遍不够。国内影响比较大的应用软件的漏洞均可用于病毒传播，如千千静听 med 文件格式堆溢出漏洞，用户使用具有漏洞的千千静听播放或者浏览包含恶意代码的 med 声音文件时，木马病毒就会轻易进入用户的计算机系统中。例如，暴风影音 II 的一个 ActiveX 控件漏洞，当安装了暴风影音 II 的用户在浏览黑客精心构造的包含恶意代码的网页后，会下载任意程序到用户系统上，并以当前用户权限自动运行。再比如联众游戏大厅 GLIEDown2.dll ActiveX 控件漏洞，当用户安装含有漏洞的联众



游戏大厅时，浏览到黑客构造的含有恶意代码的网页后，会在后台自动下载任意恶意程序，以当前用户上下文权限运行。如上所述，如果应用软件漏洞被准确利用，用户在打开一个.doc 或.pdf 文档，或者看一个视频、听一首歌曲的过程中，均可能感染上病毒。图 5.3 显示了卡巴斯基 2011 年统计的漏洞软件被在线攻击的类型分布。

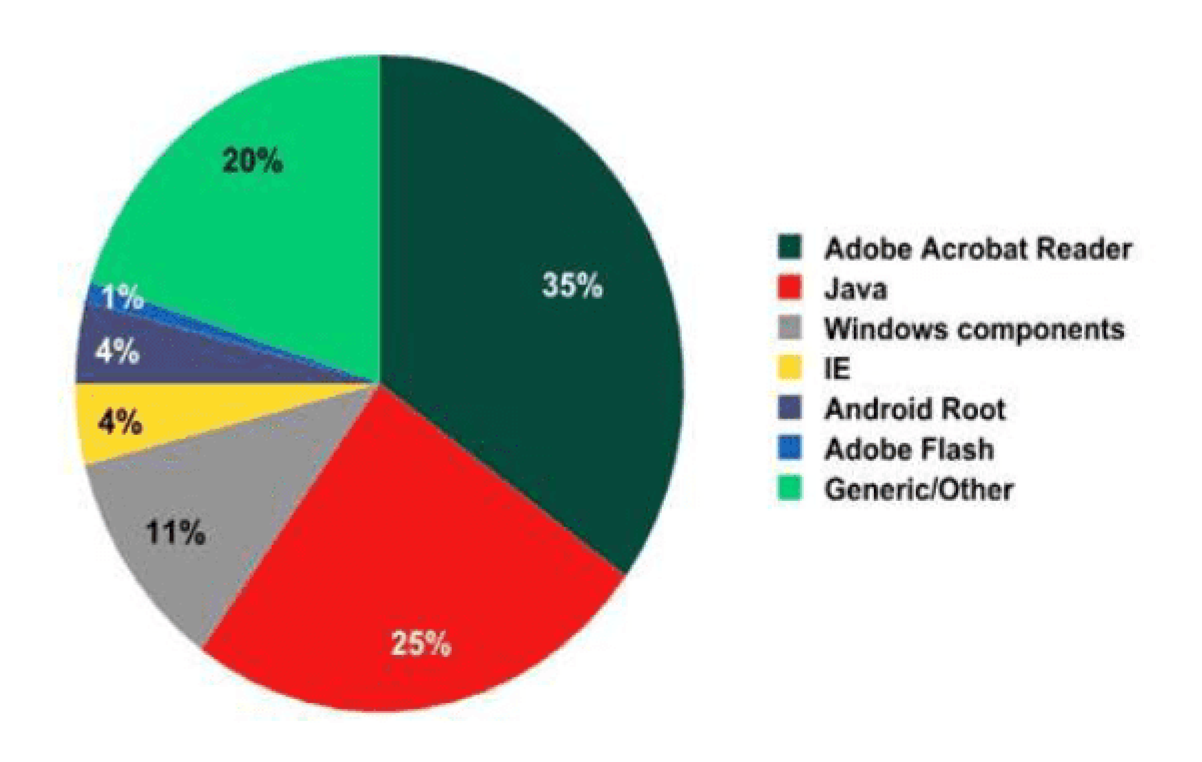


图 5.3　2011 年被在线攻击的漏洞软件分布

3. 利用系统漏洞传播病毒

这里所说的系统漏洞是指操作系统及其周边基础服务软件的漏洞。这类漏洞的特点是影响范围广且危害巨大，如在 Windows 操作系统上臭名昭著的 RPC(Remote Procedure Call)系列漏洞，至今还是许多病毒传播的重要途径。通过网络进行复制和传播的蠕虫病毒，能够利用 Windows RPC 漏洞直接感染装有 Windows 系统的主机，不需要用户进行干预，这也是网络中经常成片出现主机感染病毒的原因。不仅 RPC 漏洞危害比较大，其他在 Windows 上出现的漏洞危害都不小，如最近被发现的远程桌面协议漏洞(CVE-2012-0002)。这个漏洞允许通过 RDP 服务远程执行代码，属于高危漏洞。攻击者可能使用特别构造的一系列数据包获得对系统的完全访问。随后攻击者能够安装程序，查看、修改或是删除数据，或是创建拥有完全用户权限的新账号，当然也是用于病毒传播比较理想的渠道。

目前流行的病毒基本上都会融合多种传播方式，利用系统漏洞是其中不可或缺的一种。如“飞客”(Conficker)病毒及其多类变种，利用 Windows 操作系统 MS08-067 漏洞进行传播，同时也能借助任何有 USB 接口的硬件设备、网络共享来感染。MS08-067 漏洞就是 RPC 漏洞的一种，而不少 RPC 服务程序是默认启动的，这为利用这类漏洞的病毒提供了极大的方便。病毒会随机或按照一定的策略选择一个网段或一些 IP 地址，针对这个漏洞进行攻击，如果攻击成功就能在受害主机上复制自身，并从这台新感染的主机发起同样的攻击，一旦网络中有一定数量的主机感染了这种病毒，网络中的攻击流量就会显著上升甚至拥塞网络，IPS 等安全设备检测到这种攻击而告警内网有大量攻击也就不足为奇了。总之，Windows 等广泛应用的系统为黑客利用系统漏洞传播病毒提供了广阔的空间。

5.7.3　病毒使攻击更有针对性

漏洞评估病毒(Vulnerability Assessment Worms)已经出现，该类病毒对计算机安全漏洞进行扫描并综合评估后，将漏洞信息反馈给病毒编写者，病毒编写者再伺机进行有针对性的攻击行为。漏洞评估病毒的行为一般以信息收集为主，为黑客入侵铺路，不具有很强的

破坏性，因此对病毒扫描产品具有一定的隐匿性，通常不会轻易被反病毒软件检测到。同时，这类病毒还可能会受到病毒编写者的远程控制，会不定期地对自身进行更新，通过此方法也有可能逃过反病毒软件的查杀。随着黑客攻击越来越专业、越来越有耐心，APT(Advanced Persistent Threat，高级持续性威胁)攻击已经成为信息安全的重要威胁。可以预见，作为黑客攻击前奏的漏洞评估病毒将越来越普遍。

5.7.4 应对病毒与漏洞攻击的双重威胁

为防御更广泛而有针对性的攻击，企业需要采取立体的安全基础措施，如在内网中部署终端安全接入认证并在互联网出口及服务器入口部署入侵防御系统等，并紧密关注配置管理，及时地部署安全更新；仔细监测并进行高级分析，以便发现威胁；如果受到攻击的企业根据其所处的行业环境考虑到“由蓄谋已久的对手发起的目标攻击”这一因素，就有可能遏制攻击者的活动，从而赢得时间进行检测、响应并减轻攻击。

普通用户可以通过坚持以下基本安全原则，避免受到黑客攻击或感染病毒：认识到使用安全性较强的密码的重要性，并付诸实践；定期更新操作系统及应用软件，包括但不限于应用软件及操作系统的升级补丁；使用可信来源的软件并保持更新；谨慎地点击网页链接；谨慎对待附件和文件传输；警惕利用社交网络技术手段的恶意行为。

复习思考题五

一、填空题

1. 计算机病毒按破坏程度分类可以分为________病毒和________病毒。
2. 基于传染方式不同，计算机病毒可分为________病毒、______病毒和______病毒 3 种。
3. 按照病毒特有的算法，可以将计算机病毒划分为_________病毒、_________病毒和_________病毒。
4. 按照病毒的链接方式，可以将计算机病毒划分为_________病毒、_________病毒、_________病毒和___________病毒。
5. 网络反病毒技术包括_________、_________和_________等 3 种技术。
6. 计算机病毒传播的途径一般有_________、__________和_________3 种。

二、选择题

1. 计算机病毒是一种(　　)。

   A. 软件故障　　B. 硬件故障　　C. 程序　　D. 黑客
2. 下列不属于计算机病毒特征的是(　　)。

   A. 传染性　　B. 潜伏性　　C. 破坏性　　D. 免疫性
3. 下列属于杀毒软件的是(　　)。

   A. Microsoft Access　　B. KV3000　　C. MS-DOS　　D. Photoshop
4. 计算机病毒是一种破坏计算机功能或者毁坏计算机中所存储数据的(　　)。

   A.程序代码　　B.微生物病菌　　C.计算机专家　　D.计算机硬件
5. 木马程序一般是指潜藏在用户计算机中带有恶意性质的，利用它可以在用户不知



情的情况下窃取用户联网计算机上的重要数据信息的(　　)。

A. 远程控制软件　　B. 计算机操作系统

C. 木头做的马　　D. 计算机硬件设备

6. 网络蠕虫一般指利用计算机系统漏洞、通过互联网传播扩散的一类病毒程序，为了防止受到网络蠕虫的侵害，应当注意对(　　)进行升级更新。

A. 计算机操作系统　　B. 计算机硬件

C. 文字处理软件　　D. 杀病毒软件

7. 计算机病毒不具有(　　)特征。

A. 破坏性　　B. 隐蔽性　　C. 传染性　　D. 无针对性

8. (　　)是一种基于远程控制的黑客工具，它通常寄生于用户的计算机系统中，盗窃用户信息，并通过网络发送给黑客。

A. 文件病毒　　B. 木马　　C. 引导型病毒　　D. 蠕虫

9. (　　)是一种可以自我复制的完全独立的程序，它的传播不需要借助被感染主机的其他程序。它可以自动创建与其功能完全相同的副本，并在没人干涉的情况下自动运行。

A. 文件病毒　　B. 木马　　C. 引导型病毒　　D. 蠕虫

三、简答题

1. 什么是计算机病毒？病毒都可以通过哪些途径传播？
2. 什么是计算机网络病毒？简述计算机网络病毒的特点。
3. 简述计算机网络病毒的分类。
4. 简述计算机网络病毒的危害。
5. 简述病毒发作前的症状。
6. 常用的反病毒技术有哪些？
7. 计算机病毒发展的新技术有哪些？
8. 国内常用的杀病毒软件有哪些？

第 6 章　防火墙技术

学习目标

系统学习防火墙的基本概念与作用，防火墙的优、缺点及分类，常用的防火墙技术及防火墙的体系结构。了解在选择防火墙时应遵循的基本原则和应注意的事项及防火墙技术的发展趋势。通过本章的学习，读者应掌握以下内容：

- 掌握防火墙基本概念与作用，防火墙的优、缺点及分类，常用的防火墙技术(包过滤技术、应用代理技术、状态监视技术)，防火墙的体系结构。
- 了解选择防火墙的基本原则和注意事项，防火墙技术的发展趋势。

6.1　防火墙基本概念与分类

随着 Internet 的日益普及，有越来越多的企事业单位开始通过互联网发展业务和提供服务。然而，在互联网为企事业单位提供方便的同时，由于其自身的开放性，也带来了潜在的安全威胁。目前，黑客对网络的攻击方法已经有几千种，而且大多数具有严重的威胁性。全世界现有 20 多万个黑客网站。每当一种新的网络攻击手段出现，一周之内便可通过互联网传遍全世界。在不断扩大的计算机网络空间中，几乎到处都有黑客的踪影，无处不遭受黑客的攻击。

这些安全威胁极大地损害了人们对互联网的信心，从而影响了 Internet 发挥更大的作用。因为没有有效的安全保护，很多企事业单位放缓了将部分业务或服务转移到网上的步伐，极大地降低了工作效率。因此，如何能够为本组织的网络提供尽可能强大的安全防护就成为各企事业单位的关注焦点。在这种情况下，防火墙进入了人们的视野。

6.1.1　防火墙基本概念

1. 防火墙的概念

如果一个网络连接到 Internet，其内部用户就可以访问外部世界并与之通信，同时，外部世界也可以访问该网络并与之交互。为保证系统安全，就需要在该网络和 Internet 之间插入一个中介系统，竖起一道安全屏障，以阻挡来自外部网络对本网络的威胁和入侵，这种中介系统称为“防火墙”或“防火墙系统”。

防火墙是指设置在不同网络(如企业内部网和公共网)或网络安全域之间的一系列部件的组合，它是不同网络或网络安全域之间信息的唯一出入口，能根据企业的安全策略控制(允许、拒绝、监测)出入网络的信息流，且其本身具有较强的抗攻击能力，是提供信息安全服务、实现网络和信息安全的基础设施。

从实现方式上来看，防火墙可以分为硬件防火墙和软件防火墙两类。硬件防火墙是通过硬件和软件的结合来达到隔离内、外部网络的目的；软件防火墙则通过纯软件的方式来



实现。

从逻辑上来看，防火墙是一个分离器、一个限制器，也是一个分析器。它能有效地监控内部网和 Internet 之间的任何活动，保障内部网络的安全，防火墙示意图如图 6.1 所示。

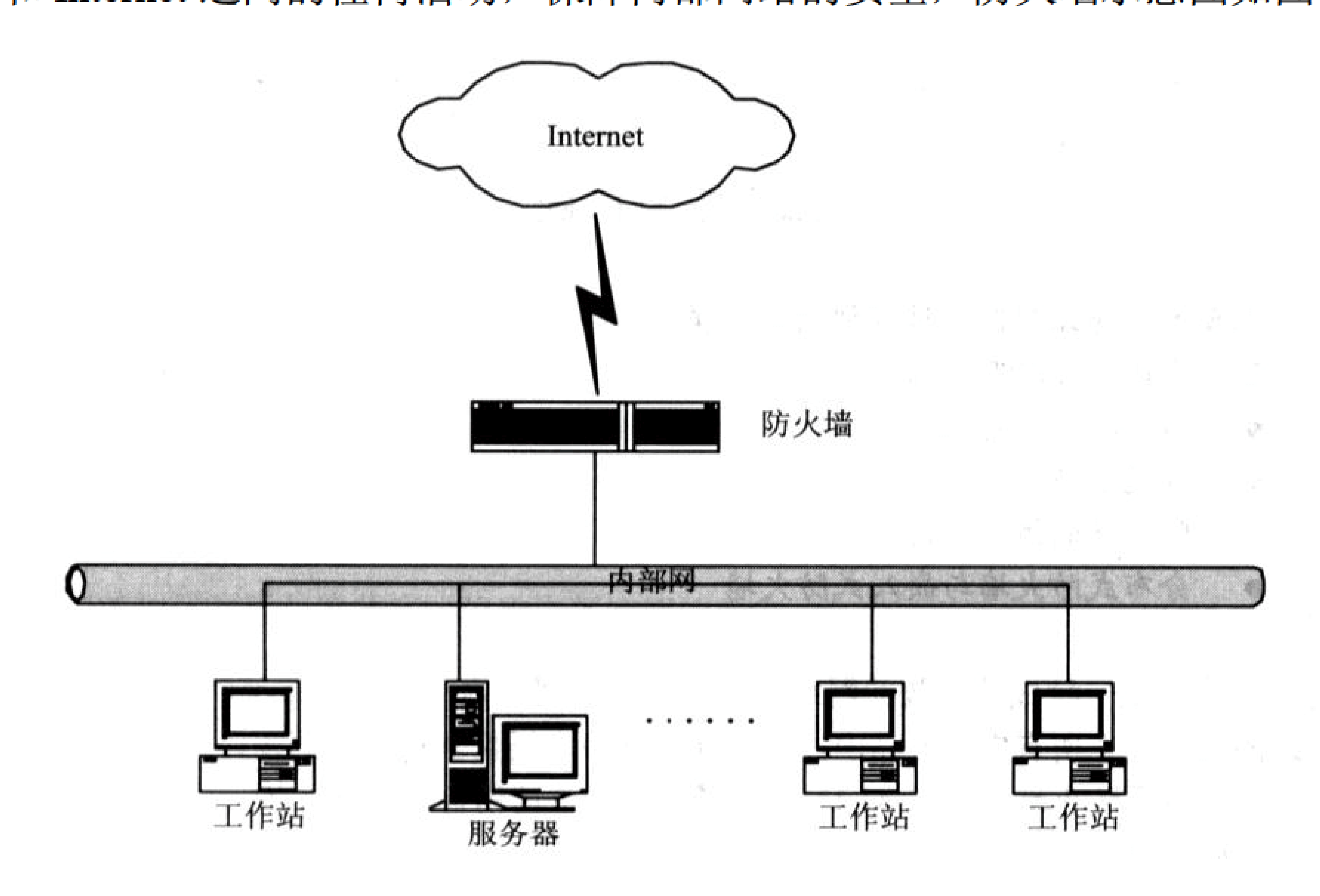


图 6.1 防火墙示意图

2. 其他概念

以下是几个有关防火墙的常用概念。

(1) 外部网络(外网)。防火墙之外的网络，一般为 Internet，默认为风险区域。

(2) 内部网络(内网)。防火墙之内的网络，一般为局域网，默认为安全区域。

(3) 包过滤。也称为数据包过滤，是依据系统事先设定好的过滤规则，检查数据流中的每个数据包，根据数据包的源地址、目标地址及端口等信息来确定是否允许数据包通过。

(4) 代理服务器。它是指代表内部网络用户向外部网络中的服务器进行连接请求的程序。

(5) 状态检测技术。这是第三代网络安全技术。状态检测模块在不影响网络安全正常工作的前提下，采用抽取相关数据的方法对网络通信的各个层次实行检测，并作为安全决策的依据。

(6) 虚拟专用网(VPN)。这是一种在公用网络中配置的专用网络。

(7) 漏洞。这是系统中的安全缺陷，漏洞可以导致入侵者获取信息并导致不正确的访问。

(8) 数据驱动攻击。入侵者把一些具有破坏性的数据藏匿在普通数据中传送到 Internet 主机上，当这些数据被激活时就会发生数据驱动攻击。例如，修改主机中与安全有关的文件，留下更容易进入系统的后门程序等。

(9) IP 地址欺骗。突破防火墙系统最常用的方法是 IP 地址欺骗，它同时也是其他一系列攻击方法的基础。入侵者利用伪造的 IP 地址发送虚假的数据包，乔装成来自内部网的数据，这种类型的攻击非常危险。



6.1.2　防火墙的作用

防火墙能够隔离风险区域与安全区域，但不会妨碍人们对风险区域的访问。防火墙的作用是监控进出网络的信息，仅让安全的、符合规则的信息进入内部网络，为用户提供一个安全的网络环境。

防火墙是加强网络安全非常流行的方法。在 Internet 上超过 1/3 的 Web 网站都是用某种形式的防火墙加以保护的，这是对黑客防范最严密、最安全的一种方式。任何关键性的服务器，都应该放在防火墙之后。

1. 防火墙的基本功能

从总体上看，防火墙应具有以下基本功能。

(1)　限制未授权用户进入内部网络，过滤掉不安全的服务和非法用户。

(2)　防止入侵者接近内部网络的防御设施，对网络攻击进行检测和报警。

(3)　限制内部用户访问特殊站点。

(4)　记录通过防火墙的信息内容和活动，为监视 Internet 安全提供方便。

2. 防火墙的特性

一个好的防火墙系统应具有以下特性。

(1)　所有在内部网络和外部网络之间传输的数据都必须通过防火墙。

(2)　只有被授权的合法数据，即防火墙安全策略允许的数据，才可以通过防火墙。

(3)　防火墙本身具有预防入侵的功能，不受各种攻击的影响。

(4)　人机界面良好，用户配置使用方便，易管理。系统管理员可以对防火墙进行设置，对 Internet 的访问者、被访问者、访问协议及访问方式进行控制。

3. 防火墙与病毒防火墙的区别

“病毒防火墙”是与网络防火墙不同范畴的软件，但由于有着“防火墙”的名字，容易引起混淆。实际上，这两种产品之间存在本质的区别。

(1)　“病毒防火墙”应该称为“病毒实时检测和清除系统”，是反病毒软件的一种工作模式。当它运行时，会把病毒监控程序驻留在内存中，随时检查系统中是否有病毒；一旦发现有携带病毒的文件，就会马上激活杀毒模块。

可以看出，病毒防火墙不是对进出网络的病毒进行监控，而是对所有的系统应用程序进行监控，由此来保障用户系统的“无毒”环境。

(2)　网络防火墙并不监控全部的系统应用程序，它只对存在网络访问的那部分应用程序进行监控。利用网络防火墙，可以有效地管理用户系统的网络应用，同时保护系统不被各种非法的网络攻击所伤害。

可以看出，网络防火墙的主要功能是预防黑客入侵，防止木马盗取机密信息。病毒防火墙是一种反病毒软件，主要功能是查杀本地病毒、木马。两者具有不同的功能，在安装反病毒软件的同时应该安装网络防火墙。



6.1.3 防火墙的优、缺点

1. 优点

防火墙是加强网络安全的一种有效手段，它有以下优点。

(1) 防火墙能强化安全策略。Internet 上每天都有上百万人在浏览信息，不可避免地会有一些恶意用户试图攻击别人，防火墙充当了防止攻击现象发生的“警察”，它执行系统规定的安全策略，仅允许符合规则的信息通过。

(2) 防火墙能有效地记录 Internet 上的活动。因为所有进出内部网络的信息都必须通过防火墙，所以防火墙能记录被保护的内部网络和不安全的外部网络之间发生的各种事件。

(3) 防火墙是一个安全策略的检查站。所有进出内部网络的信息都必须通过防火墙，防火墙便成为一个安全检查站，把可疑的访问拒之门外。

2. 缺点

防火墙并不是万能的，安装了防火墙的系统仍然存在着安全隐患。以下是防火墙的一些缺点。

(1) 不能防范恶意内部用户。防火墙可以禁止内部用户经过网络发送机密信息，但用户可以将数据复制到磁盘上带出去。如果入侵者已经进入防火墙内部，防火墙同样无能为力。内部用户可以不经过防火墙窃取数据、破坏硬件和软件，这类攻击占了全部攻击的一半以上。

(2) 不能防范不通过防火墙的连接。防火墙能够有效地防范通过它传输的信息，却不能防范不通过它传输的信息。例如，如果站点允许对防火墙后面的内部系统进行拨号访问，那么防火墙绝对没有办法阻止入侵者进行拨号入侵。

(3) 不能防范全部的威胁。防火墙被用来防范已知的威胁，性能良好的防火墙设计方案可以防范某些新的威胁，但没有一个防火墙能自动防御所有新的威胁。

(4) 防火墙不能防范病毒。防火墙不能防范从网络上传染来的病毒，也不能消除计算机已存在的病毒。无论防火墙多么安全，都需要用户有一套防毒软件来防范病毒。

6.1.4 防火墙分类

防火墙的分类方式有很多种。根据受保护的对象不同，可以分为网络防火墙和单机防火墙；根据防火墙主要部分的形态不同，可以分为软件防火墙和硬件防火墙；根据防火墙使用的对象不同，可以分为企业级防火墙和个人防火墙；根据防火墙检查数据包的位置不同，可以分为包过滤防火墙、应用代理防火墙和状态检测防火墙。

1. 网络防火墙和单机防火墙

网络防火墙是指用来保护某个网络安全的防火墙，目前的防火墙大都是网络防火墙。

单机防火墙主要是为了保护单独主机而设计的防火墙。

一般说来，为了保护网络中的主机安全，人们大多选用网络防火墙。但对于网络中一些重要的主机，也需要给它们加装单机防火墙。



2. 软件防火墙和硬件防火墙

软件防火墙是指防火墙的所有组件都为软件，不需要专用的硬件设备，Check Point 公司的 Firewall-1 就是这样一种防火墙。而硬件防火墙则需要专用的硬件设备，目前国内的防火墙基本上属于这一类型。

3. 企业级防火墙和个人防火墙

企业级防火墙主要为企业上网服务。它能够进行复合分层保护，支持大规模本地和远程管理，同时和 VPN 相结合，从而扩展了安全联网基础设施，并且可以应用于大规模网络。这类防火墙提供了功能强大、操作灵活的认证功能，允许企业配置它们对现有的数据库进行安全传送，并且充分利用网络带宽，提供负载均衡的能力。

而个人防火墙主要是为了防护个人的主机，一般就是前面所述的单机防火墙。其功能一般较简单。

4. 包过滤防火墙、应用代理防火墙和状态检测防火墙

这种分类方法是最主要、最基本的一种分类方法。其分类依据是防火墙检查点的位置。

(1) 包过滤防火墙是在网络层对数据包进行选择，选择的依据是系统内设置的访问控制表(Access Control Table)。通过检查数据流中每个数据包的源地址、目的地址、所用的端口号、协议状态等因素或其组合，来确定是否允许该数据包通过。这种防火墙逻辑简单，价格便宜，易于安装和使用，网络性能和透明性好。然而，非法访问一旦突破防火墙，即可对主机上的软件和配置漏洞进行攻击；同时，数据包的源地址、目的地址以及 IP 的端口号都在数据包的头部，很有可能被窃听或假冒。

(2) 应用代理防火墙是内网与外网的隔离点，能够监视和隔绝应用层通信流，同时也常结合包过滤器功能。应用代理防火墙工作在 OSI 模型的最高层，掌握着应用系统中可用作安全决策的全部信息。此类防火墙的安全性比包过滤防火墙高，但它的效率则相对较低。

(3) 状态检测防火墙把包过滤的快速性和应用代理的安全性很好地结合在一起，目前已经是防火墙最流行的检测方式。

状态检测防火墙试图跟踪通过防火墙的网络连接和包，这样防火墙就可以使用一组附加的标准，以确定允许或拒绝通信。状态检测防火墙是在使用了基本包过滤防火墙的通信基础上应用一些技术来做到这一点的。

状态检测防火墙不仅跟踪包中包含的信息，还能够记录有用的信息以帮助识别包，如已有的网络连接、数据的传出请求等。

状态检测防火墙可截断所有传入的通信，而允许所有传出的通信。因为防火墙跟踪内部出去的请求，所有按要求传入的数据被允许通过，直到连接被关闭为止。只有未被请求的传入通信被截断。

6.2 防火墙技术

随着防火墙技术的不断发展，目前应用的防火墙技术主要有包过滤技术、应用代理技术和状态监视技术等。



6.2.1 包过滤技术

1. 包过滤技术简介

包过滤(Packet Filtering)技术依据系统事先设定好的过滤规则，检查数据流中的每个包，根据包头信息来确定是否允许数据包通过，并拒绝发送可疑的数据包。

使用包过滤技术的防火墙叫作包过滤防火墙(Packet Filter)，因为它工作在网络层，又叫网络层防火墙(Network Level Firewall)。

包过滤技术的依据是分包传输技术。网络上的数据都是以包为单位进行传输的，数据被分割成一定大小的包，每个包分为包头和数据两部分，包头中含有源地址和目的地址等信息。路由器从包头中读取目的地址并选择一条物理线路发送出去，当所有的包抵达后会在目的地重新组装还原。

包过滤防火墙一般由屏蔽路由器(Screening Router，也称为过滤路由器)来实现，这种路由器在普通路由器的基础上加入 IP 过滤功能，是防火墙最基本的构件，包过滤防火墙工作原理如图 6.2 所示。

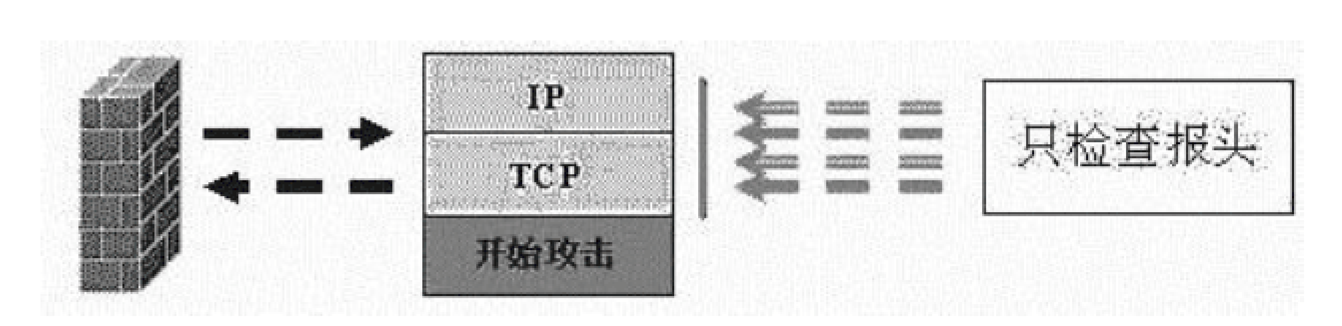


图 6.2 包过滤防火墙工作原理

包过滤防火墙读取包头信息，与信息过滤规则相比较，按顺序检查规则表中的每一条规则，直至发现包中的信息与某条规则相符。如果有一条规则不允许发送某个包，路由器就将它丢弃；如果有一条规则允许发送某个包，路由器就将它发送；如果没有任何一条规则能符合，路由器就会使用默认规则，一般情况下，默认规则就是禁止该包通过。

屏蔽路由器是一种价格较高的硬件设备。如果网络不是很大，可以由一台 PC 装上相应的软件(如 KarlBridge、DrawBridge)来实现包过滤功能。

2. 包过滤防火墙的优点

包过滤防火墙具有明显的优点。

(1) 一个屏蔽路由器能保护整个网络。一个恰当配置的屏蔽路由器连接内部网络与外部网络，进行数据包过滤，就可以取得较好的网络安全效果。

(2) 包过滤对用户透明。包过滤不要求任何客户机配置，当屏蔽路由器决定让数据包通过时，它与普通路由器没什么区别，用户感觉不到它的存在。较强的透明度是包过滤的一大优势。

(3) 屏蔽路由器速度快、效率高。屏蔽路由器只检查包头信息，一般不查看数据部分，而且某些核心部分是由专用硬件实现的，故其转发速度快、效率较高，通常作为网络安全的第一道防线。

3. 包过滤防火墙的缺点

(1) 屏蔽路由器的缺点也是很明显的，通常它不保存用户的使用记录，这样就不能从

访问记录中发现黑客的攻击记录。

(2) 配置烦琐也是包过滤防火墙的一个缺点。没有一定的经验，是不可能将过滤规则配置完美的。有些的时候，因为配置错误，防火墙根本就不起作用。

(3) 包过滤的另一个弱点就是不能在用户级别上进行过滤，只能认为内部用户是可信任的、外部用户是可疑的。

(4) 单纯由屏蔽路由器构成的防火墙并不十分安全，一旦屏蔽路由器被攻陷就会对整个网络产生威胁。

4. 包过滤防火墙的发展阶段

(1) 第一代：静态包过滤防火墙。第一代包过滤防火墙与路由器同时出现，实现了根据数据包头信息的静态包过滤，这是防火墙的初级产品。静态包过滤防火墙对所接收的每个数据包审查包头信息，以便确定其是否与某一条包过滤规则相匹配，然后做出允许通过或者拒绝通过的决定。

(2) 第二代：动态包过滤(Dynamic Packet Filter)防火墙。此类防火墙采用动态设置包过滤规则的方法，避免了静态包过滤所存在的问题。动态包过滤只有在用户的请求下才打开端口，并且在服务完毕后关闭端口，从而降低受到与开放端口相关的攻击的可能性。防火墙可以动态地决定哪些数据包可以通过内部网络的链路和应用程序层服务，用户可以配置相应的访问策略，只有在允许范围内才自动打开端口，当通信结束时关闭端口。

这种方法在两个方向上都将暴露端口的数量减少到最小，给网络提供更高的安全性。对于许多应用程序协议而言，如媒体流，动态 IP 包过滤提供了处理动态分配端口的最安全方法。

(3) 第三代：全状态检测(Stateful Inspection)防火墙。第三代包过滤类防火墙采用状态检测技术，在包过滤的同时，检查数据包之间的关联性，检查数据包中动态变化的状态码。它有一个监测引擎，能够抽取有关数据，从而对网络通信的各层实施监测，并动态地保存状态信息作为以后执行安全策略的参考。当用户访问请求到达网关的操作系统前，状态监视器要抽取有关数据进行分析，结合网络配置和安全规定作出接纳、拒绝、身份认证、报警或给该通信加密等操作。

状态检测防火墙保留状态连接表，并将进出网络的数据当成一个个会话，利用状态表跟踪每一个会话状态。状态监测对每一个包的检查不仅根据规则表，更考虑了数据包是否符合会话所处的状态，因此提供了完整的对传输层的控制能力。

状态检测技术在大大提高安全防范能力的同时也改进了流量处理速度，使防火墙性能大幅度提升，因而能应用在各类网络环境中，尤其是在一些规则复杂的大型网络上。

(4) 第四代：深度包检测(Deep Packet Inspection)防火墙。状态检测防火墙的安全性得到了一定程度的提高，但是在对付 DDoS(分布式拒绝服务)攻击、实现应用层内容过滤、病毒过滤等方面的表现还不能尽如人意。

面对新形势下的蠕虫病毒、DDoS 攻击、垃圾邮件泛滥等严重威胁，最新一代包过滤防火墙采用了深度包检测技术。深度包检测技术融合入侵检测和攻击防范两方面功能，不仅能深入检查信息包，查出恶意行为，还可以根据特征检测和内容过滤，来寻找已知的攻击，同时能阻止异常访问。深度包检测引擎以基于指纹匹配、启发式技术、异常检测及统



计学分析等技术来决定如何处理数据包。深度包检测防火墙能阻止 DDoS 攻击、病毒传播和高级应用入侵等问题。

6.2.2 应用代理技术

1. 代理服务器简介

代理服务器(Proxy Server)是指代表内网用户向外网服务器进行连接请求的服务程序。代理服务器运行在两个网络之间，它对于客户机来说像是一台真正的服务器，而对于外网的服务器来说，它又是一台客户机。

代理服务器的基本工作过程是，当客户机需要使用外网服务器上的数据时，首先将请求发给代理服务器，代理服务器再根据这一请求向服务器索取数据，然后再由代理服务器将数据传输给客户机。

同理，代理服务器在外部网络向内部网络申请服务时也发挥了中间转接的作用，代理防火墙工作原理如图 6.3 所示。

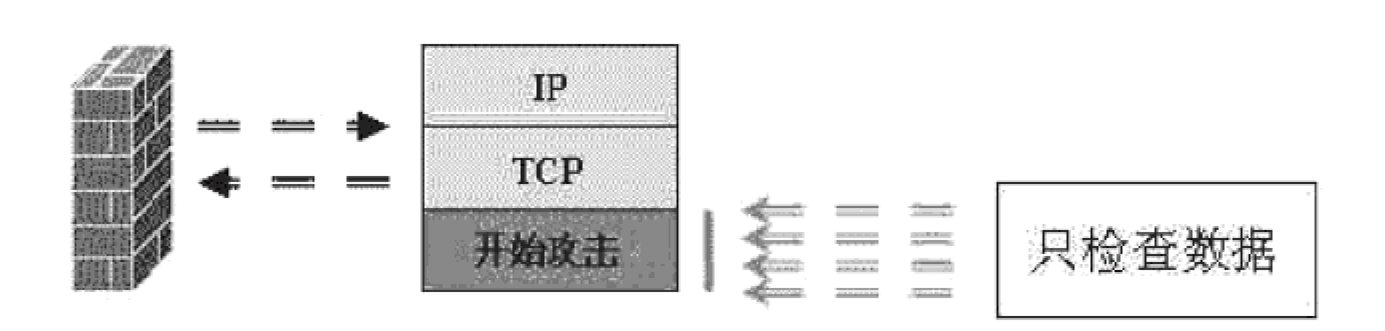


图 6.3　代理防火墙工作原理示意图

内网只接受代理服务器提出的服务请求，拒绝外网的直接请求。当外网向内网的某个节点申请某种服务(如 FTP、Telnet、WWW 等)时，先由代理服务器接受，然后代理服务器根据其服务类型、服务内容、被服务的对象等，决定是否接受此项服务。如果接受，就由代理服务器向内网转发这项请求，并把结果反馈给申请者。

可以看出，由于外部网络与内部网络之间没有直接的数据通道，外部的恶意入侵也就很难伤害到内网。

代理服务器通常拥有高速缓存，缓存中存有用户经常访问站点的内容，在下一个用户要访问同样的站点时，服务器就不必重复读取同样的内容，既节约了时间也节约了网络资源。

2. 应用代理的优点

(1) 应用代理易于配置。因为代理是一个软件，所以比过滤路由器容易配置。如果代理实现得好，可以对配置协议要求较低，从而避免了配置错误。

(2) 应用代理能生成各项记录。因代理在应用层检查各项数据，所以可以按一定准则让代理生成各项日志、记录。这些日志、记录对于流量分析、安全检验是十分重要和宝贵的。

(3) 应用代理能灵活、完全地控制进出信息。通过采取一定的措施，按照一定的规则，可以借助代理实现一整套的安全策略，控制进出信息。

(4) 应用代理能过滤数据内容。可以把一些过滤规则应用于代理，让它在应用层实现过滤功能。



3. 应用代理的缺点

(1) 应用代理速度比路由器慢。路由器只是简单查看包头信息，不作详细分析、记录；而代理工作于应用层，要检查数据包的内容，按特定的应用协议对数据包内容进行审查、扫描，并转发请求或响应，故其速度比路由器慢。

(2) 应用代理对用户不透明。许多代理要求客户端作相应改动或定制，因而增加了不透明度。为内部网络的每一台主机安装和配置特定的客户端软件既耗费时间，又容易出错。

(3) 对于每项服务，应用代理可能要求不同的服务器。因此可能需要为每项协议设置一个不同的代理服务器，挑选、安装和配置所有这些不同的服务器是一项繁重的工作。

(4) 应用代理服务通常要求对客户或过程进行限制。除了一些为代理而设置的服务外，代理服务器要求对客户或过程进行限制，每一种限制都有不足之处，人们无法按他们自己的步骤工作。由于这些限制，代理应用就不能像非代理应用那样灵活运用。

(5) 应用代理服务受协议弱点的限制。每个应用层协议，都或多或少存在一些安全隐患，对于一个代理服务器来说，要彻底避免这些安全隐患几乎是不可能的，除非关掉这些服务。

(6) 应用代理不能改进底层协议的安全性。

4. 应用代理防火墙的发展阶段

(1) 应用层代理(Application Proxy)。应用层代理也被为应用层网关(Application Level Gateway)，这种防火墙的工作方式同包过滤防火墙的工作方式具有本质区别。

代理服务是运行在防火墙主机上的、专门的应用程序或者服务器程序。应用层代理为某个特定应用服务提供代理，它对应用协议进行解析并解释应用协议的命令。根据其处理协议的功能可分为 FTP 网关型防火墙、Telnet 网关型防火墙、WWW 网关型防火墙等。

(2) 电路层代理(Circuit Proxy)。另一种类型的代理技术称为电路层网关(Circuit Gateway)，也称为电路级代理服务器。在电路层网关中，包被提交到用户应用层处理。电路层网关用来在两个通信的终点之间转换包。

在电路层网关中，可能要安装特殊的客户机软件，用户需要一个可变接口来相互作用或改变他们的工作习惯。

电路层代理适用于多个协议，但无法解释应用协议，需要通过其他方式来获得信息。所以，电路级代理服务器通常要求修改用户程序。其中，套接字服务器(Sockets Server)就是电路级代理服务器。套接字(Sockets)是一种网络应用层的国际标准。当内网客户机需要与外网交互信息时，在防火墙上的套接字服务器检查客户的 UserID、IP 源地址和 IP 目的地址，经过确认后，套接字服务器才与外部的服务器建立连接。对用户来说，内网与外网的信息交换是透明的，感觉不到防火墙的存在，这是因为 Internet 用户不需要登录到防火墙上。但是客户端的应用软件必须支持 Socketsifide API，内部网络用户访问外部网所使用的 IP 地址也都是防火墙的 IP 地址。

(3) 自适应代理(Adaptive Proxy)。应用层代理的主要问题是速度慢，支持的并发连接数有限。因此，NAI 公司在 1998 年又推出了具有自适应代理特性的防火墙。

自适应代理不仅能维护系统安全，还能够动态“适应”传送中的分组流量。它能根据具体需求，定义防火墙策略，而不会牺牲速度或安全性。如果对安全要求较高，则最初的



安全检查仍在应用层进行，保证实现传统代理防火墙的最大安全性。而一旦代理明确了会话的所有细节，其后的数据包就可以直接经过速度更快的网络层。

自适应代理可以和安全脆弱性扫描器、病毒安全扫描器和入侵检测系统之间实现更加灵活的集成。作为自适应安全计划的一部分，自适应代理将允许经过正确验证的设备在安全传感器和扫描器发现重要的网络威胁时，根据防火墙管理员事先确定的安全策略，自动“适应”防火墙级别。

6.2.3 状态检测技术

1. 状态检测技术简介

状态监视(Stateful Inspection)是由 CheckPoint 公司于 1993 年提出的，它是防火墙技术的一项突破性变革，把包过滤的快速性和代理的安全性很好地结合在一起，目前已经是防火墙最流行的检测方式。状态检测技术克服了以上两种技术的缺点，引入了 OSI 全 7 层监测能力，同时又能保持 Client/Server 的体系结构，也即对用户访问是透明的。

与包过滤防火墙相比，状态检测防火墙判断的依据也是源 IP 地址、目的 IP 地址、源端口、目的端口和通信协议等。与包过滤防火墙不同的是，状态检测防火墙是基于会话信息做出决策的，而不是包的信息；状态检测防火墙验证进来的数据包时，判断当前数据包是否符合允许的会话，并在状态表中保存这些信息。状态检测防火墙还能阻止基于异常 TCP 的网络层的攻击行为。网络设备，比如路由器，会将数据包分解成更小的数据帧，因此，状态检测设备通常需要将 IP 数据帧按其原来顺序组装成完整的数据包。状态检测防火墙工作原理如图 6.4 所示。

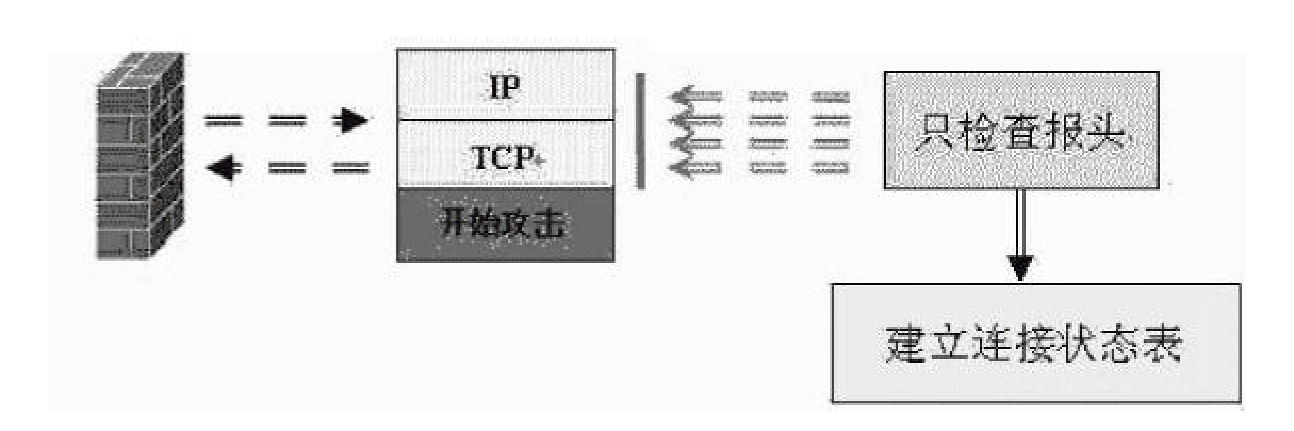


图 6.4 状态检测防火墙工作原理示意图

状态检测的根本思想是对所有网络数据建立“连接”的概念，既然是连接，必然是有一定顺序的，通信两边的连接状态也是按一定顺序进行变化的，就像打电话，一定要先拨号对方电话才能振铃。防火墙的状态检测就是事先确定好连接的合法过程模式，如果数据过程符合这个模式，则说明数据是合法的，否则就是非法数据，应该丢弃。

以下以面向连接的 TCP 协议为例来做具体说明。

TCP 协议是一个标准的面向连接协议，在真正通信前，必须按一定协议先建立连接，连接建立好后才能通信，通信结束后释放连接。连接建立过程称为 3 次握手，发起方先发送带有 SYN 标志的数据包到目的方，如果目的方端口允许连接，就会回应一个带 SYN 和 ACK 的标志，发起方收到后再发送一个只带 ACK 标志的数据包到目的方，目的方收到后就可认为连接已经正确建立。在正常断开时，一方会发送带 FIN 标志的数据包到对方，表示本方已经不会再发送数据了，但还可以接收数据，对方接收后还可以发送数据，发送完后也会发送带 FIN 标志的数据包，双方进入断开状态，经过一段时间后连接彻底删除。如

有异常情况则会发送 RST 标志的包来执行异常断开，而不论是在连接开始还是通信或断开过程。

由此可见，TCP 的连接过程是一个有序过程，新连接一定是通过 SYN 包来开始的，如果防火墙里没有相关连接信息，就收到非 SYN 包，则该包一定是非法的，可以将其扔掉；数据通信过程是有方向性的，一定是发起方发送 SYN，接收方发送 SYN ACK，不是此方向的数据就是非法的，由此状态检测可以实现 A 可以访问 B 而 B 却不能访问 A 的效果。一个连接可以用协议、源地址、目的地址、源端口、目的端口等 5 元组来唯一确定。

2. 状态检测防火墙的优点

状态检测防火墙的优点如下。

(1) 检查 IP 包的每个字段的能力，并遵从基于包中信息的过滤规则。

(2) 识别带有欺骗性源 IP 地址包。

(3) 状态检测防火墙是两个网络之间访问的唯一来源，因为所有的通信必须通过防火墙。

(4) 基于应用程序信息验证一个包的状态，如基于一个已经建立的 FTP 连接并允许返回的 FTP 包通过。

(5) 基于应用程序信息验证一个包的状态，如允许一个先前认证过的连接继续与被授予的服务通信。

(6) 记录通过的每个包的详细信息。防火墙用来确定包状态的所有信息都可以被记录，包括应用程序对包的请求、连接的持续时间、内部和外部系统所做的连接请求等。

3. 状态检测防火墙的缺点

状态检测防火墙唯一的缺点就是所有这些记录、测试和分析工作可能会造成网络连接的某种迟滞，特别是在同时有许多连接激活的时候，或者是有大量的过滤网络通信的规则存在时更是如此。

4. 状态检测防火墙的发展阶段

1) 状态检测防火墙

状态检测防火墙(Stateful Inspection Firewall)又称动态包过滤防火墙，它在网络层由一个检查引擎截获数据包并抽取出与应用层状态有关的信息，并以此作为依据决定对该数据包是接受还是拒绝。检查引擎能自动生成动态的状态信息表，并对后续的数据包进行检查，一旦发现任何连接的参数有意外变化，该连接就被中止。

状态检测防火墙克服了包过滤防火墙和应用代理服务器的局限性，能够根据协议、端口及源地址、目的地址的具体情况决定是否允许数据包通过。对于每个安全策略允许的请求，状态检测防火墙启动相应的进程，可以快速地确认符合授权流通标准的数据包，这使得其本身的运行非常快速。

2) 深度检测防火墙

深度检测防火墙(Deep Inspection Firewall)将状态检测和应用防火墙技术结合在一起，以处理应用程序的流量，防范目标系统免受各种复杂的攻击。由于结合了状态检测的所有功能，因此深度检测防火墙能够对数据流量迅速完成网络层级别的分析，并做出访问控制



决策；对于允许的数据流，根据应用层级别的信息，对负载做出进一步的决策。

状态检测技术在大力提高安全防范能力的同时也改进了流量处理速度。状态监测技术采用了一系列优化技术，使防火墙性能大幅度提升，能应用在各类网络环境中，尤其是在一些规则复杂的大型网络上。深度检测技术对数据包头或有效载荷所封装的内容进行分析，从而引导、过滤和记录基于 IP 的应用程序和 Web 服务通信流量，其工作并不受协议种类和应用程序类型的限制。采用深度检测技术，企业网络可以获得性能上的大幅度提升而无须购买昂贵的服务器或是其他安全产品。

现在使用的防火墙多是几种技术的集成，即复合型防火墙。复合型防火墙是指综合了状态检测与透明代理的新一代的防火墙，它基于 ASIC 架构，把防病毒、内容过滤融合到防火墙中，其中还包括 VPN、IDS 功能，多单元融为一体，是一种新的突破，体现了网络与信息安全的新思路。它在网络边界实施 OSI 第 7 层的内容扫描，实现了实时在网络边缘部署病毒防护、内容过滤等应用层服务措施。

复合型防火墙工作原理如图 6.5 所示。

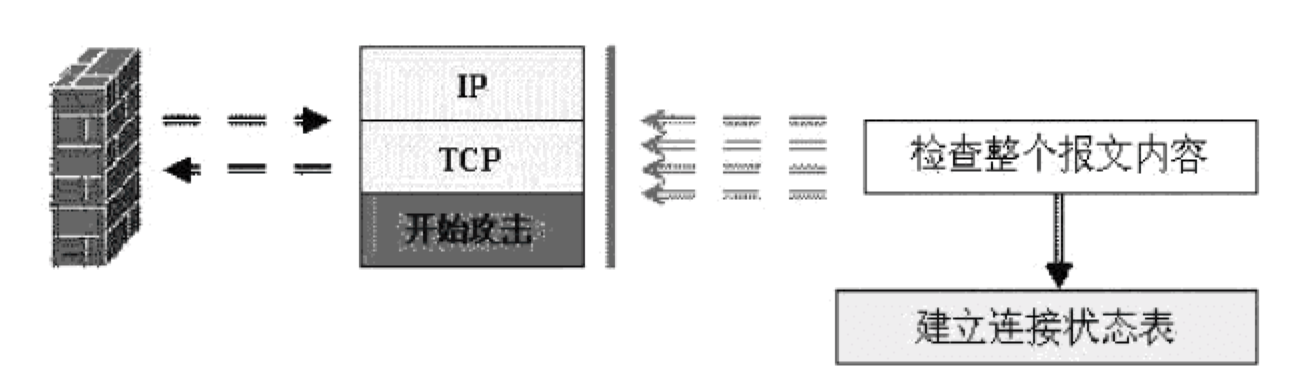


图 6.5 复合型防火墙工作原理示意图

6.2.4 技术展望

随着防火墙技术的发展，未来的防火墙将向以下几个方向发展。

(1) 分布式防火墙。

(2) 嵌入式防火墙。

(3) 深度防御。

(4) 主动防御。

(5) 与其他安全技术联动，从而产生互操作协议。

(6) 专用化，小型化，硬件化。

为达成上述防火墙发展目标，人们对新的防火墙技术有以下的一些展望。

1. 深度防御技术

深度防御技术是指防火墙在整个协议栈上建立多个安全检查点，利用各种安全手段对经过防火墙的数据包进行多次检查，从而提高防火墙的安全性。举例来说，在网络层，过滤掉所有的源路由分组和假冒 IP 源地址的分组；在传输层，遵循过滤规则过滤掉所有禁止出入的协议报文和有害数据包，如 Nuke 包、圣诞树包等；在应用层，利用 FTP、SMTP 等各种网关，控制和监测 Internet 提供的可用服务。

深度防御技术科学地混合了现有防火墙中已经广泛使用的各种安全技术(包过滤、应用网关等)，因而具有很大的灵活性和安全性。



2. 区域联防技术

以前的防火墙仅在内外网交界处进行安全控制，一旦黑客攻破该点，整个网络就暴露在黑客面前。随着黑客技术的不断提升，防火墙主机也受到越来越大的安全威胁，所以传统的防火墙结构已渐渐不能适应今天的企业架构。

新型的防火墙必须是分布式的，它结合主机型防火墙与个人计算机型防火墙，再配合传统型防火墙的功能，让其各司其职，从而形成全方位的最佳效能比的防卫架构，也就是利用“区域联防”技术。其目的是利用各区域的加强防卫动作来化解攻击行为。凡是能联入 Internet 的各终端，不管是网络主机还是服务器或个人计算机等，都应该有一定的防护功能，以避免成为黑客入侵的漏洞。

3. 网络安全产品的系统化

随着防火墙的广泛使用，人们也不断地发现防火墙的局限性。与此同时，各种各样的网络安全产品被不断地推出。因此如何能使网络安全产品组成一个以防火墙为核心的网络安全体系也是业界比较关心的技术问题。

在以防火墙为核心的网络安全体系中，防火墙和其他网络安全产品对被保护网络中出现的安全问题发出联动的反应，从而最大限度地发挥各个网络安全产品的优势，提高被保护网络的安全性。

例如，一般情况下，内外网交界的位置是网络传输的瓶颈，为了降低网络传输延迟，只有必须置于这个位置的设备(如防火墙、病毒检测设备等)才会被放置在这里，其他设备(如IDS)只能置于其他位置。而在实际使用中，IDS 的任务往往不仅在于检测入侵行为，很多时候还需要对发现的入侵行为及时地做出反应。显然，这时候需要防火墙来执行切断入侵连接的动作。

除了 IDS 之外，防火墙还可以和 VPN、病毒检测设备等进行联动，充分发挥各自的长处，协同配合，共同建立一个有效的安全防范体系。

4. 管理的通用化

管理通用化是建立一个有效的安全防范体系的必要条件。如要使各个不同的网络安全产品能够联动地做出反应，就必须让它们都使用同一种通用的“语言”，也就是发展一种它们都能够理解的协议。如此一来，不管是对防火墙还是对 IDS、VPN、病毒检测设备等网络安全设备进行操作，都可以使用通用的网络设备管理方法。

5. 专用化和硬件化

在网络应用越来越普遍的形势下，一些专用防火墙概念也被提了出来，单向防火墙(又叫网络二极管)就是其中的一种。单向防火墙的目的是让信息的单向流动成为可能，也就是网络上的信息只能从外网流入内网，而不能从内网流入外网，从而起到安全防范作用。

同时，将防火墙中部分功能固化到硬件中，也是当前防火墙技术发展的方向。通过这种方式，可以提高防火墙中瓶颈部分的执行速度，缩短防火墙导致的网络延时。



6.3 防火墙的体系结构

最简单的防火墙是一台屏蔽路由器(Screening Router)，一旦此类防火墙的屏蔽路由器被攻陷，就会对整个网络安全产生威胁，所以一般不会使用这种结构。实际上防火墙的体系结构多种多样，目前使用的防火墙大都采用以下几种体系结构。

(1) 双重宿主主机结构。

(2) 屏蔽主机结构。

(3) 屏蔽子网结构。

6.3.1 双重宿主主机结构

双重宿主主机(Dual-Homed Host)又称堡垒主机(Bastion Host)，是一台至少配有两个网络接口的主机，它可以充当与这些接口相连的网络之间的路由器，在网络之间发送数据包。一般情况下，双重宿主主机的路由功能是被禁止的，因而能够隔离内部网络与外部网络之间的直接通信，从而起到保护内部网络的作用。

双重宿主主机结构如图 6.6 所示，一般是用一台装有两块网卡的堡垒主机做防火墙。两块网卡各自与内部网络和外部网络相连。堡垒主机上运行着防火墙软件，可以转发应用程序、提供服务等。

双重宿主主机结构防火墙的最大特点是 IP 层的通信是被阻止的，两个网络之间的通信可通过应用层数据共享或应用层代理服务来完成。代理服务能够为用户提供更为方便的访问手段，也可以通过共享应用层数据来访问外网。

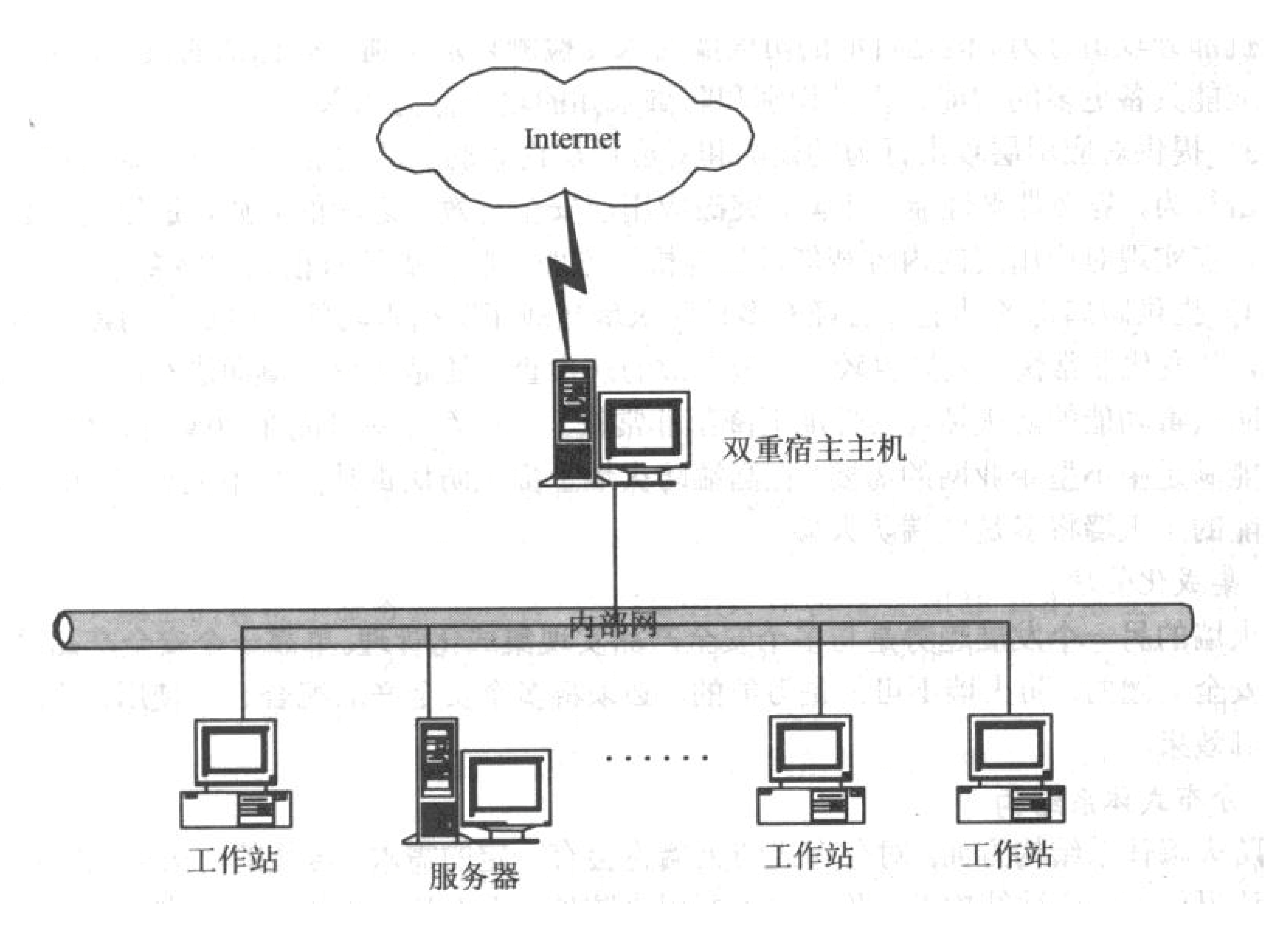


图 6.6 双重宿主主机结构示意图

双重宿主主机用两种方式来提供服务：一种是用户直接登录到双重宿主主机上来提供服务；另一种是在双重宿主主机上运行代理服务器。

第一种方式需要在双重宿主主机上开立许多账号，这是很危险的，原因如下。

(1)　用户账号的存在会给入侵者提供相对容易的入侵通道，每一个账号通常有一个可重复使用的口令(即通常用的口令和一次性口令相对)，这样很容易被入侵者破解。

(2)　如果双重宿主主机上有很多账号，管理员维护起来很麻烦。

(3)　支持用户账号会降低机器本身的稳定性和可靠性。

(4)　因为用户的行为是不可预知的，如双重宿主主机上有很多用户账户，这会给入侵检测带来很大的麻烦。

如果在双重宿主主机上运行代理服务器，产生的问题相对要少得多，而且一些服务本身的特点就是“存储转发”型的。当内网的用户要访问外部站点时，必须先经过代理服务器认证，然后才可以通过代理服务器访问因特网。

双重宿主主机是唯一的隔开内部网和 Internet 之间的屏障，如果入侵者得到了双重宿主主机的访问权，内部网络就会被入侵，所以为了保证内部网络的安全，双重宿主主机应具有强大的身份认证系统，才可以阻挡非法登录。

双宿主机防火墙优于屏蔽路由器之处在于，堡垒主机的系统软件可用于维护系统日志，这对日后的安全检查很有用。

双重宿主主机防火墙的一个致命弱点是，一旦入侵者侵入堡垒主机并使其具有路由功能，则任何外网用户均可以随便访问内网。

堡垒主机是用户的网络上最容易受侵袭的机器，要采取各种措施来保护它。设计时有两条基本原则：①堡垒主机要尽可能简单，保留最少的服务，关闭路由功能；②随时做好准备，修复受损害的堡垒主机。

6.3.2　屏蔽主机结构

屏蔽主机结构(Screened Host Gateway)，又称主机过滤结构。屏蔽主机结构需要配备一台堡垒主机和一个有过滤功能的屏蔽路由器，其示意图如图 6.7 所示。屏蔽路由器连接外部网络，堡垒主机安装在内部网络上。通常在路由器上设立过滤规则，并使堡垒主机成为从外部网络唯一可直接通过的主机。入侵者要想入侵内部网络，必须越过屏蔽路由器和堡垒主机两道屏障，所以屏蔽主机结构要比双重宿主主机结构具有更好的安全性和可用性。

堡垒主机是外网主机连接到内部网络的桥梁，并且仅有某些确定类型的连接被允许(如传送进来的电子邮件)。任何外部网络如果要试图访问内部网络，必须连接到这台堡垒主机上。因此，堡垒主机需要有较高的安全等级。

在屏蔽路由器中数据包过滤可以按下列之一配置。

(1)　允许其他的内部主机为了某些服务(如 Telnet)与外网主机连接。

(2)　不允许来自内部主机的所有连接(强迫主机必须经过堡垒主机使用代理服务)。

用户可以针对不同的服务混合使用这些手段，某些服务可以被允许直接经由数据包过滤，而其他服务可以被允许仅间接地经过代理，这完全取决于用户实行的安全策略。

在采用屏蔽主机防火墙的情况下，过滤路由器是否正确配置是安全与否的关键。过滤路由器的路由表应当受到严格的保护，如果路由表遭到破坏，数据包就不会被路由到堡垒主机上，从而使外部访问越过堡垒主机进入内网。



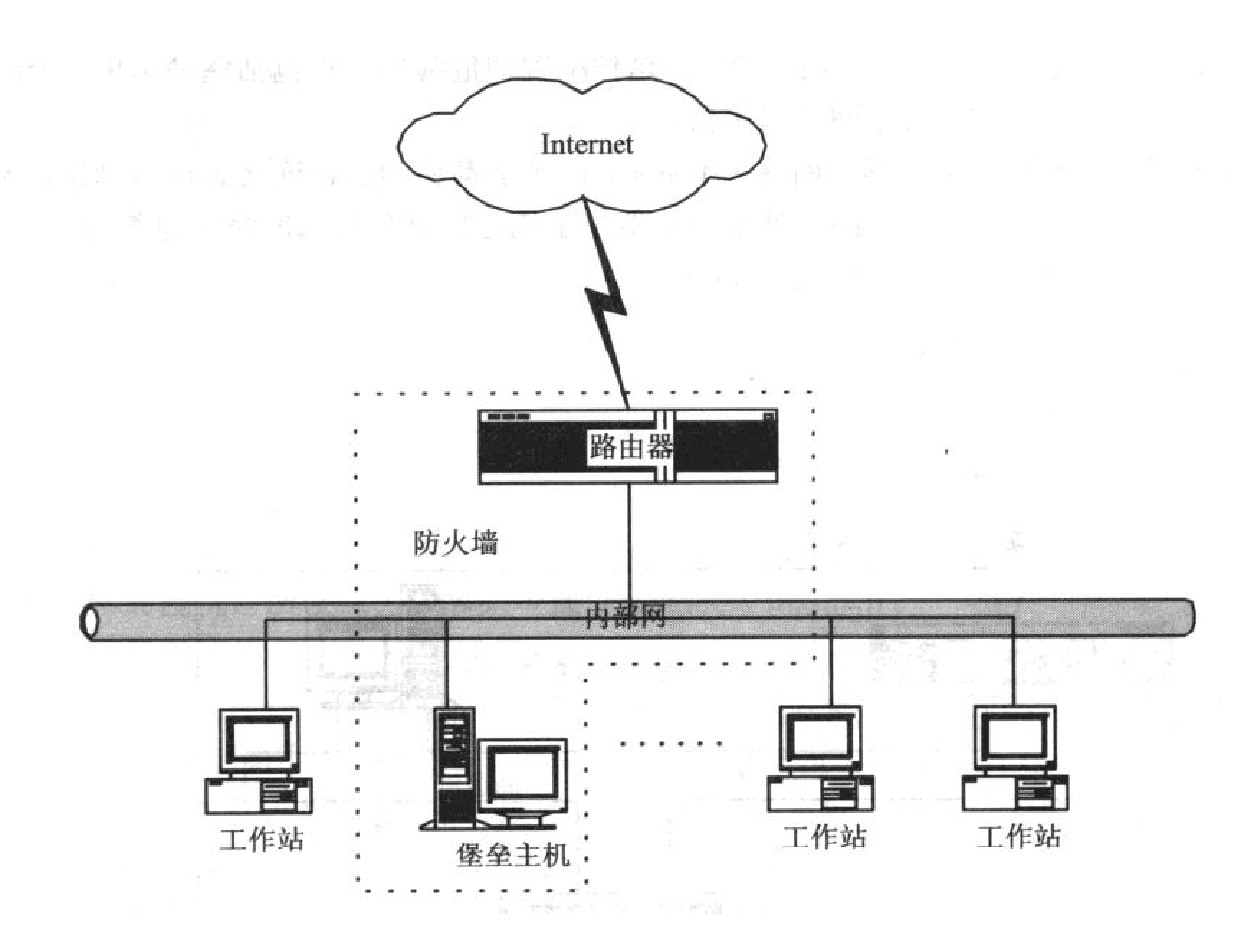


图 6.7　屏蔽主机结构示意图

屏蔽主机结构的缺点是，如果入侵者有办法侵入堡垒主机，而且在堡垒主机和其他内部主机之间没有任何安全保护措施的情况下，整个网络对入侵者是开放的。为了改善这一状况，可以使用屏蔽子网。

6.3.3　屏蔽子网结构

堡垒主机是内部网络上最容易受攻击的目标，在屏蔽主机结构中，如果能够侵入堡垒主机，就可以毫无阻挡地进入内部网络。因为该结构中屏蔽主机与其他内部机器之间没有特殊的防御手段，内部网络对堡垒主机不做任何防备。

屏蔽子网结构(Screened Subnet)可以改善这种状况，它是在屏蔽主机结构的基础上添加额外的安全层，即通过添加周边网络(即屏蔽子网)进一步把内部网络与外部网络隔离开。

一般情况下，屏蔽子网结构包含外部和内部两个路由器。两个屏蔽路由器放在子网的两端，在子网内构成一个“非军事区”(DMZ)。有的屏蔽子网中还设有一台堡垒主机作为唯一可访问点，支持终端交互或作为应用网关代理。这种配置的危险地带仅包括堡垒主机、子网主机及所有连接内网、外网和屏蔽子网的路由器。

屏蔽子网结构最常见的形式如图 6.8 所示，通过在周边网络上用两个屏蔽路由器隔离堡垒主机，能减少堡垒主机被侵入的危害程度。外部路由器保护周边网络和内部网络免受来自 Internet 的侵犯，内部路由器保护内部网络免受来自 Internet 和周边网的侵犯。要侵入使用这种防火墙的内部网络，入侵者必须要通过两个屏蔽路由器。即使入侵者能够侵入堡垒主机，内部路由器也会阻止他继续入侵内部网络。

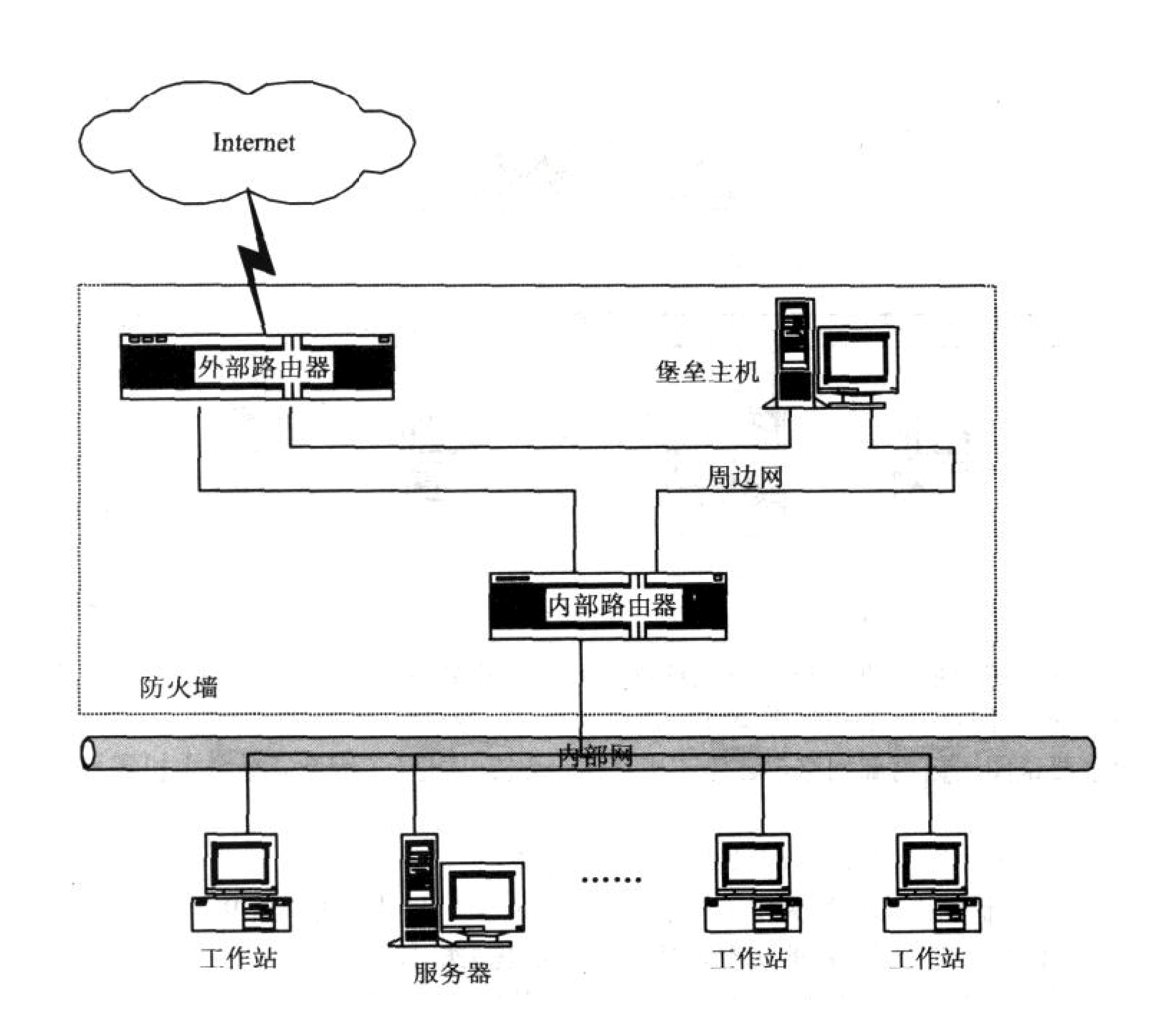


图 6.8　屏蔽子网结构示意图

6.3.4　防火墙的组合结构

组建防火墙时，一般很少采用单一结构，通常采用多种结构的组合。这种组合主要取决于网管中心向用户提供什么样的服务，以及网管中心能接受什么等级的风险。采用哪种技术还取决于经费、投资的大小或技术人员的技术水平、时间等因素。

防火墙的组合结构一般有以下几种形式。

(1)　使用多堡垒主机。

(2)　合并内部路由器与外部路由器。

(3)　合并堡垒主机与外部路由器。

(4)　合并堡垒主机与内部路由器。

(5)　使用多台内部路由器。

(6)　使用多台外部路由器。

(7)　使用多个周边网络。

(8)　使用双重宿主主机与屏蔽子网。

6.4　选择防火墙的注意事项

6.4.1　选择防火墙的基本原则

作为一类比较成熟的安全产品，市场上已经有很多种品牌的防火墙产品，如 Check Point 的 FireWall-1、Cisco 的 PIX、Network Associate 的 Gauntlet Firewall、Netscreen 的 Netscreen-10/100/1000 Firewall 等。每一类防火墙都有其独特的功能特点和技术个性。例如，



Check Point 的 GUI 界面是一大特色，Cisco 以性能好而著名、NAI 以独特的技术出名、Netscreen 以性能和简单易用性而为人称道等，这些防火墙都有自己的定位。再加上国内的品牌，如此众多的防火墙产品让用户眼花缭乱，不同种类的防火墙的实现技术细节也各不相同，而且在产品宣传上引进很多新的概念和术语，使用户很难选择。

一般说来，选择防火墙时的基本原则如下。

(1) 明确自己的安全和功能需求，从而决定所期望的防火墙产品的安全性、功能和性能。

(2) 明确投资范围和标准，以此来衡量防火墙的性价比。

(3) 在相同的基准和条件下，比较不同防火墙的各项指标和参数。

(4) 综合考虑自己的安全管理人员的经验、能力和技术素质，考察防火墙产品的管理和维护的手段和方式。

(5) 根据实际应用的需求，了解防火墙附加功能的定义，以及日常系统的维护手段和策略。

考虑以上基本因素后，针对自己的具体需求，然后选择合适于自己环境和需求的防火墙产品。

虽然防火墙在当今 Internet 上的存在是有生命力的，但它不能替代其他的安全措施，它并不是解决所有网络安全问题的万能药方，只是网络安全政策和策略中的一个基本组成部分。

6.4.2 选择防火墙的注意事项

防火墙作为一种系统和网络安全的主要手段，其定位是实现网络边界的访问控制，阻止来自外部的攻击和破坏。因此，选择防火墙产品，首先要考察它的主要安全功能和特性，然后才是其他的功能和特点。

1. 防火墙自身是否安全

作为一种安全设备，防火墙的本职功能就是安全功能，因此，衡量和选择防火墙首先要考虑的就是它的安全性。目前，防火墙的实现技术有三种：包过滤、应用代理、状态检测，另外也有三者的混合技术。传统的观念是应用代理最安全、包过滤最不安全，这种描述不一定准确；应该是应用代理的控制最细，包过滤的控制最粗；关键要看这种控制是否适合用户的网络环境和安全需要。

在客户端环境中，防火墙系统和厂商的防火墙产品是不同的，防火墙系统包括了防火墙产品、防火墙的运行平台和环境、防火墙安全控制策略、防火墙的审计策略及防火墙的管理手段等；而防火墙产品只是防火墙系统中的一个重要组成部分，也就是厂商提供的部分。防火墙系统的安全性和防火墙产品的安全性不是等同的。一般来说，厂商所说的防火墙的安全性是指产品本身的安全性，而不等同于客户环境下防火墙系统的安全性；各个评测机构所说的哪个防火墙最安全，指的是测试环境下防火墙系统的安全性，它体现了防火墙的合理、坚固、安全配置的安全性，包含了测试安装人员的经验和技术。

防火墙的实现方式有两种：一种是基于专用硬件和操作系统的硬件防火墙；另一种是基于商用操作系统的防火墙。

对基于商用操作系统的防火墙系统，安全性包括操作系统本身的安全性、防火墙的安全性、配置和策略的合理性及管理的安全性等。一般来说商用操作系统本身并不是为防火墙的安全目的而设计的，它是通用的，能提供各类服务，而且有大量的安全补丁可供下载，Internet 上对它的攻击方式也最多。要保证此类防火墙系统的安全，不但必须花大量的时间来加固防火墙运行的操作系统的安全性，在投入运行后，还要时刻关注新补丁的出现并及时修补。对于这一类防火墙，对用户的要求也比较高，要求用户要熟悉操作系统的各个方面。

对基于专用硬件和操作系统的防火墙系统，安全性只和防火墙产品及安全策略相关。操作系统是专门为防火墙而设计的，充分地考虑了操作系统的安全，无须打补丁和加固。这一类防火墙的安全性只与管理有关。

对于客户来说，所需要的是防火墙系统的安全性，而不是防火墙产品本身的安全性。但只有保证了防火墙产品本身的安全性，才能进一步实现防火墙系统的安全性。

2. 防火墙是否具有很好的性能

防火墙的性能包含以下几个方面的指标。

(1) 防火墙的并发连接数。和同时访问的用户数有关。

(2) 防火墙的数据包速率。每秒数据包转发速率，与数据包的大小有关。

(3) 防火墙的转发速率。每秒通信吞吐量。

(4) 防火墙的延时。由于防火墙带来的通信延时。

衡量防火墙性能的基准是与没有防火墙时的网络相比较，即直接连接通信时的比较。

影响防火墙系统的性能相关因素有以下几个方面。

(1) 防火墙产品。

(2) 防火墙所运行的硬件环境。

(3) 防火墙的安全策略。

(4) 防火墙的附加功能等。

对基于商用操作系统的防火墙产品来说，直接与运行的硬件平台和操作系统相关。由于商用操作系统和硬件并不是专门为防火墙而设计的，因而它是通用平台。要保证这一类防火墙的高性能，需要对操作系统的软、硬件配置进行优化，使之适合于防火墙的应用。防火墙的硬件与内存、硬盘、CPU 等有关；对基于硬件的防火墙系统，其性能与所选用的型号和部署的安全策略有关。

例如，并发连接数是防火墙最常见的参数，在厂家的产品说明书中，大家经常可以看到，从低端设备的 500 个并发连接，一直到高端设备的数十万个并发连接，存在着巨大的差异。那么，什么是并发连接数？是不是并发连接数越大的防火墙越好？(最大)并发连接数指的是防火墙或代理服务器对其业务信息流的处理能力，是防火墙能够同时处理的点对点连接的最大数目，它反映防火墙对多个连接的访问控制能力和连接状态跟踪能力。这个参数的大小能直接影响到防火墙所能支持的最大信息点数。

并发连接表是防火墙用以存放并发连接信息的地方，由启动后的防火墙在内存空间中动态分配，该表的大小就是防火墙所能支持的最大并发连接数。

但过大的并发连接表会带来以下负面影响。



(1) 消耗大量的内存空间。

(2) 在相同的数据结构和搜索方式下，会增大防火墙系统对表项的搜索时间，增加防火墙对报文处理的转发延迟。

(3) 不考虑客户网络客观情况而盲目增大系统并发连接表，会造成表空间及内存资源的大量闲置浪费。

(4) 由于并发连接表对内存的占用，会造成防火墙系统本身得不到足够的内存资源；虽然虚拟内存可以解决内存的紧张问题，但虚拟内存依赖硬盘与内存页之间的数据映射切换，在读写速度上难以与物理内存相提并论。

防火墙的性能永远和投资有关系，只有在同样的投资情况下比较防火墙的性能才是合理的。防火墙系统的性能和投资成正比，和策略数、策略的复杂性、功能成反比。

3. 防火墙是否稳定

就一个成熟的产品来说，系统的稳定性是最基本的要求。如果防火墙尚未最后定型，或未经过严格测试就被推向市场，其稳定性就很难保证。防火墙的稳定性从厂商的宣传材料中是看不出来的，但可以从以下几个渠道获得。

(1) 国家权威的测评认证机构，如公安部计算机安全产品检测中心和中国国家信息安全测评认证中心等。

(2) 与其他产品相比，是否获得更多的国家权威机构的认证、推荐和入网证明。

(3) 考察某防火墙是否已经有了使用单位，其用户量大小，以及用户们对于该防火墙的评价。如有可能，最好咨询一下那些对稳定性要求较高的重要单位的用户，如政府机关、国家部委、证券或银行系统、军队等。

(4) 自己试用。先在自己的网络上进行一段时间的试用(一个月左右)，如果在试用期间时常有死机现象，这种产品就可以完全不用考虑了。

(5) 厂商开发研制的历史。这也是一个重要指标，一般来说，如果没有两年以上的开发经历恐怕难以保证产品的稳定性。

(6) 厂商的实力。其包括注册资金、技术开发人员、市场销售人员和技术支持人员多少等。相信一家注册资金几百万，人员不超过20～30人的公司是不可能保证产品稳定性的。

4. 防火墙是否可靠

防火墙的安全定位是控制不同网络之间的访问，而不是隔断网络，因此可靠性对防火墙类访问控制设备来说尤为重要，其直接影响受控网络的可用性。尤其是关键业务的网络，网络的通畅是第一的，不允许由于防火墙而导致的对网络畅通性的影响。

防火墙系统的可靠性和防火墙的组成有关，是各个组件的可靠性的综合。对基于通用平台的防火墙系统，可靠性和运行的主机硬件、操作系统、防火墙软件本身有关。在这类防火墙系统中，系统的不可靠因素比较多；对基于专用硬件和操作系统的防火墙系统的组件比较少，不可靠因素相对少一些。

5. 防火墙的管理是否简便

对于防火墙类访问控制设备，除安全控制不断调整外，业务系统访问控制的调整也很频繁，这些都要求防火墙的管理在充分考虑安全需要的前提下，尽可能提供方便、灵活的

管理方式和方法。防火墙系统的管理要考虑管理的易用性、简单性和可用性。对于大型企业来说，对管理的重视程度更高。管理的内容有日常维护、防火墙的配置、策略制定、监控、日志和报告等。

目前，防火墙系统的管理特性有以下几点。

(1) 集中管理、配置、监控和报告。

(2) 组模式管理，复用配置和策略信息。

(3) 安全的远程管理。

(4) 基于浏览器管理。

(5) GUI 管理界面。

(6) 防火墙的日常维护和审计。

6. 防火墙是否易用

防火墙的易用性与客户的投资价值直接相关，易用性主要从网络安全管理的日常工作着手，主要表现在以下几个方面。

(1) 是否易于安装和部署，充分考虑防火墙系统对原有网络的改动和影响，衡量这种工作量的负担和复杂性。

(2) 是否易于日常使用，是否会影响最终用户的使用，是否会影响用户的日常使用习惯等。

(3) 防火墙系统是否易于日常维护。

7. 防火墙是否可以抵抗拒绝服务攻击

在当前的网络攻击中，拒绝服务攻击使用频率最高，它可以分为两类。

(1) 由于操作系统或应用软件本身设计或编程上的缺陷造成的，由此带来的攻击种类很多，只有通过打补丁的办法加以解决。

(2) 由于 TCP/IP 协议本身的缺陷造成的，虽然只有少数的几种，但危害性非常大。

要求防火墙解决第一类攻击显然是强人所难。系统缺陷和病毒不同，没有病毒码可以作为依据，因此在判断到底是不是攻击时常常出现误报，目前国内外的入侵检测产品对这类攻击至少有 50%的误报率。而且这类攻击检测产品不能装在防火墙上，否则防火墙可能把合法的报文误认为是攻击。防火墙能做的是对付第(2)类攻击。

抵抗拒绝服务攻击是防火墙的基本功能之一，目前有很多防火墙号称可以抵御拒绝服务攻击，实际上它只能降低拒绝服务攻击的危害，而不是抵御这种攻击。因此在采购防火墙时，应该详细考察这一功能的真实性和有效性。

8. 防火墙是否具有可扩展性、可升级性

目前市面上的防火墙一般标配 3 个网络接口，分别接外部网、内部网和 SSN。因此，在购买防火墙时必须问清楚，是否可以增加网络接口，因为有些防火墙只支持 3 个接口，不具有扩展性。

随着用户业务的扩展、网络技术的发展以及黑客攻击手段的变化，防火墙也必须不断地升级，所以要充分考虑防火墙系统是否能够升级。防火墙系统的升级包括运行平台的升级和防火墙软件本身的升级。一般要求升级工作量和复杂性不要太大。



选择升级时，一般应考虑以下几个方面。

(1) 升级方式：远程或本地。

(2) 升级工作量。

(3) 升级复杂性。

(4) 升级对运行中的防火墙系统的影响。

(5) 是否可以集中升级。

(6) 是否需要重新安装。

(7) 升级程序是否自动化。

(8) 是否需要重新配置。

9. 防火墙是否能适应复杂环境

在防火墙基本功能和安全性满足要求的情况下，还要考虑对于复杂网络的适应性。国内许多网络没有首先考虑安全性的问题，而是先运行网络，然后考虑增加安全设备。所以存在很多这样的现象：先建网络，后增加防火墙。这势必给防火墙提出了一个要求——让防火墙去适应各种各样的网络环境。例如，在已经运行的网络中，对外开放的服务器采用客户机/服务器结构，将与之通信的外网 IP 地址做到应用程序中，此时，要求防火墙支持透明模式。如果服务器处于 DMZ(非军事区)区域，同时，单位局域网用户又有上网需求，同时隐藏 IP。这时，内网和外网采用路由模式，而 DMZ 区服务器和外网采用透明模式。整个防火墙工作是既有路由又有透明的混合工作模式。这本来需要两个防火墙完成的工作，就可以由支持混合模式的防火墙来完成。

另外，对于大型的网络来说，防火墙能否通过简单的配置，实现复杂网络的安全需求。对于用户、IP、服务都可以定义相应的组，从而简化了安全规则数目。

10. 防火墙是否具备 AAA 和日志功能

随着网络安全的发展以及用户对网络安全认识的不断深入，AAA(认证、授权、记账)已经不可避免地融入防火墙。现在用户对 AAA 的要求越来越高，已经远远超越了简单的用户名/口令认证阶段，逐步走向全面、标准的 AAA。从目前校园网和某些科研机构的应用来看，防火墙必须在框架设计阶段就考虑到 AAA，而且必须提供相应的工具，使防火墙的 AAA 系统与用户原有的认证系统平滑过渡。

如何有效地使用和管理防火墙日志，是许多国内厂商没有解决的问题。经过这几年的发展，人们逐渐意识到产品标准化、国际化是大势所趋。目前，多数国内防火墙厂商使用 Oracle、SQL Server 等商业数据库进行日志管理，出现了两头不靠的尴尬局面：一方面对于中小型用户，商业数据库提高了总体成本和管理难度；另一方面对于大型企业用户，一般防火墙厂商提供的日志分析管理软件，又达不到企业级应用的要求。目前，现实的做法是向第三方工业标准靠齐，比如 Webtrends 的 WELF，提供给用户简单快捷、行之有效的解决问题办法，并且使大型企业用户可以使用专业的第三方防火墙日志分析软件。现在，国外许多厂商，如 Netscreen、Checkpoint 都宣布支持这个格式，国内有些厂商也已经实现对这个格式的支持，如龙马卫士防火墙的日志就是完全采用 WELF 格式实现的。



11. 防火墙是否支持 VPN 功能

VPN 是一种安全传输技术，它是在公网上实现私有专用网的一种方式。目前越来越多的企业对 VPN 提出应用的需求，而很多的防火墙产品也都开始支持 VPN 功能，在选择 VPN 时应注意以下几个因素。

(1) VPN 实现技术和标准的符合程度。

(2) VPN 模块的兼容性。

(3) VPN 的性能指标。

(4) 配置 VPN 的简单性。

(5) 加密算法的强度和可用性。

12. 防火墙是否具备附加功能

防火墙的基本功能是保护网络的安全，但是安全是一个整体的架构，在这个架构下还包含有其他种类的安全技术，很多防火墙产品本身融合了许多其他的功能和技术。在选择这些附加功能时，首先要考虑的是哪些功能是防火墙必要的，哪些功能是我们必要的，哪些功能是可有可无的。

一般来说，防火墙所带的附加功能有以下几个方面。

(1) VPN 功能。

(2) 带宽管理功能。

(3) 网络计费功能。

(4) URL 过滤功能。

(5) 日志分析功能。

(6) 内容扫描功能。

(7) 防病毒功能。

上述大部分附加功能是给第三方厂家提供接口，通过第三方的解决方案实现的。在选择这些附加功能时，必须和整个企业安全架构相关联，选择必要的附加功能。

6.5　访问控制列表

6.5.1　访问控制列表的基本概念

访问控制列表(Access Control List，ACL)，也称为访问列表(Access List)，它最直接的功能就是包过滤。通过访问控制列表 ACL 可以在路由器、3 层交换机上进行网络安全属性配置，可以实现对进入到路由器、3 层交换机的输入数据流进行过滤。

访问控制列表的主要作用有以下两个。

(1) 限制路由更新。控制路由更新信息发往什么地方，同时希望在什么地方收到路由更新信息。

(2) 限制网络访问。为了确保网络安全，通过定义规则限制用户访问一些服务(如只需要访问 WWW 和电子邮件服务，其他服务如 Telnet 则禁止)，或只允许一些主机访问网络



等。如图 6.9 所示，通过在路由器上设置 ACL，从而控制内网用户只能访问外部 Internet，而不能访问 FTP 服务器。

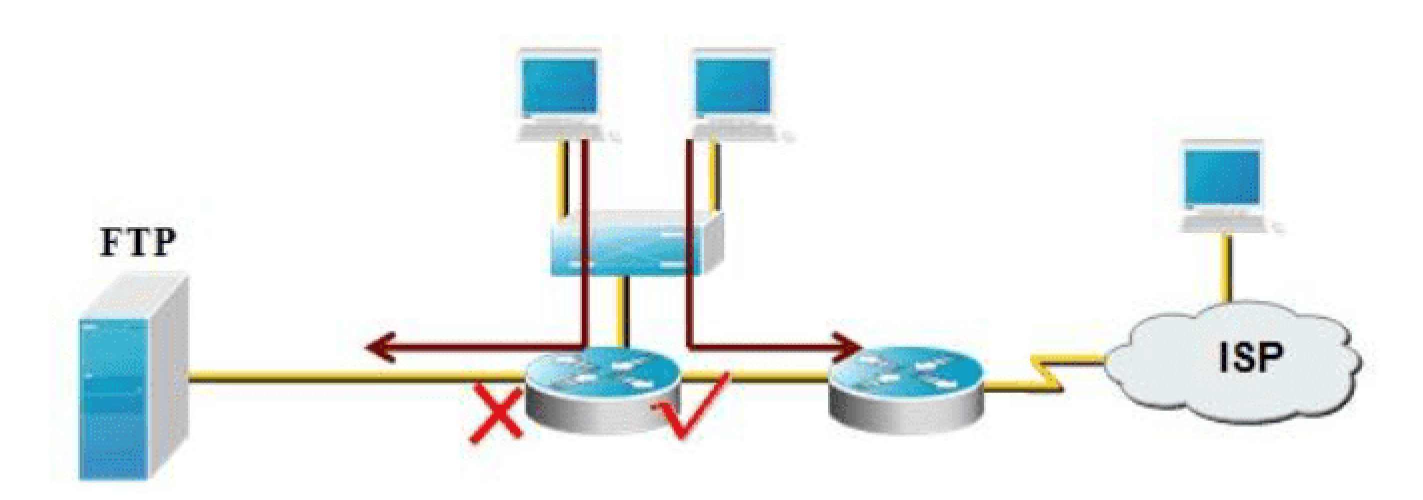


图 6.9　用访问控制列表限制网络访问

过滤输入数据流的定义可以基于网络地址、TCP/UDP 的应用等。可以选择对于符合过滤标准的流是丢弃还是转发，因此必须知道网络是如何设计的，以及路由器接口是如何在过滤设备上使用的。要通过 ACL 配置网络安全属性，只有通过命令完成配置。

创建访问列表时，定义的准则将应用于路由器上所有的分组报文，路由器通过判断分组是否与准则匹配来决定是否转发或阻断分组报文。

6.5.2　访问控制列表的定义

访问控制列表的定义分为两步：第一步，定义规则(哪些数据允许通过，哪些不允许)；第二步，将规则应用在设备接口上。

对于单一的访问控制列表来说，可以使用多条独立的访问控制列表语句来定义多种准则，其中所有的语句引用同一个编号，以便将这些语句绑定到同一个访问控制列表。但使用的语句越多，阅读和理解访问控制列表就越困难。

在每个访问控制列表的末尾隐含一条“拒绝所有数据流”的准则语句，因此如果分组与任何准则都不匹配，将被拒绝。

加入的每条准则都被追加到访问控制列表的最后，一旦语句被创建后，就无法单独删除它，而只能删除整个访问控制列表。所以访问控制列表语句的次序非常重要。路由器在决定转发还是阻断分组时，路由器按语句创建的次序将分组与语句进行比较，找到匹配的语句后便不再检查其他准则语句。

ACL 的基本准则有以下几条(图 6-10)。

(1)　一切未被允许的就是禁止的。

(2)　路由器默认允许所有的信息流通过。

(3)　防火墙默认封锁所有的信息流，对希望提供的服务逐项开放。

(4)　按规则链来进行匹配，如使用源地址、目的地址、源端口、目的端口、协议、时间段进行匹配。

(5)　从头到尾、自顶向下的匹配方式。

(6)　匹配成功马上停止。

(7)　立刻使用该规则的“允许、拒绝……”。

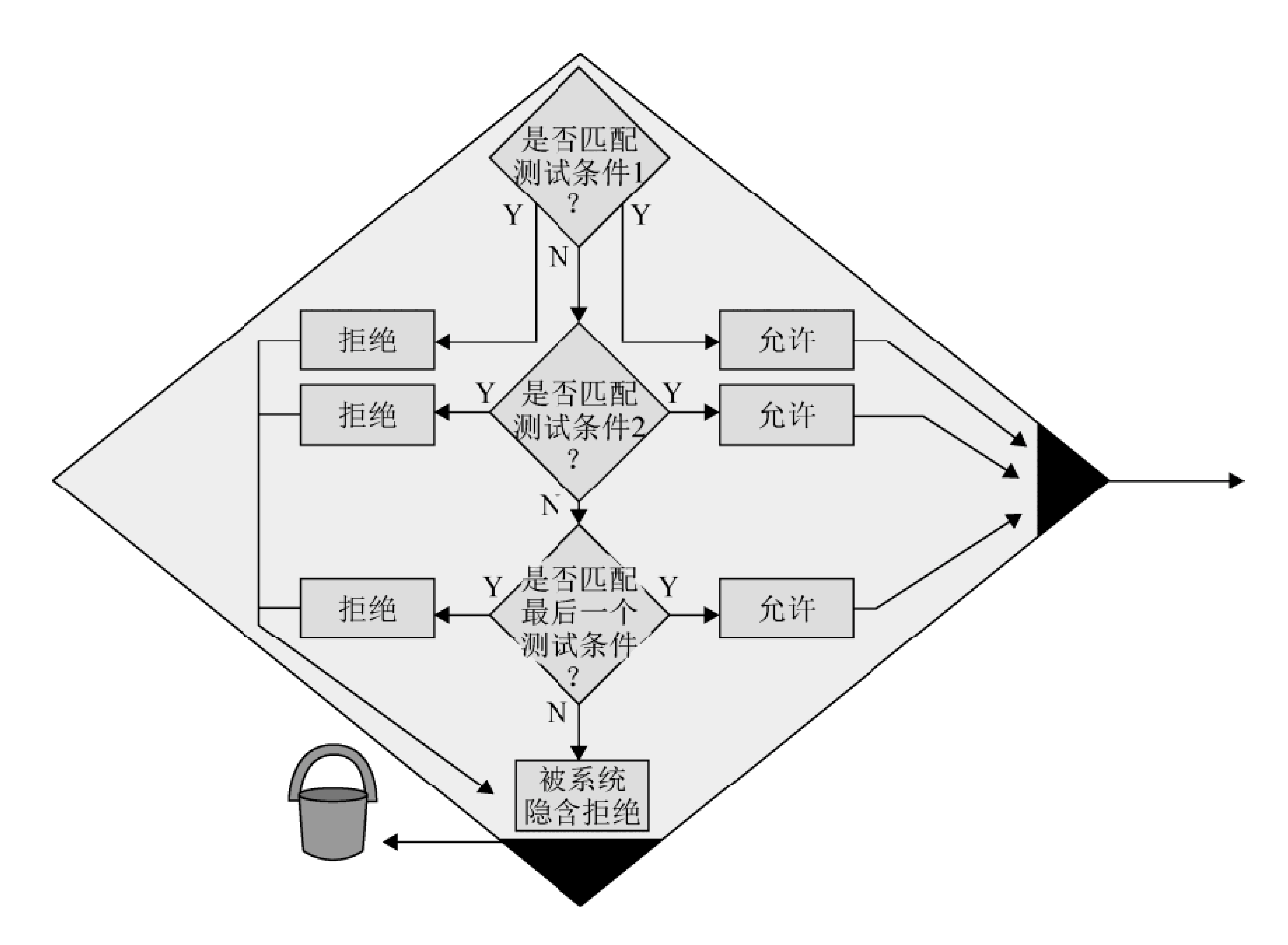


图 6.10　ACL 的基本准则

6.5.3　访问控制列表的类型

ACL 的类型主要分为 IP 标准访问控制列表(Standard IP ACL)和 IP 扩展访问控制列表(Extended IP ACL)，每一条 ACL 必须指定唯一的名称或编号，标准 ACL 的编号范围为 1～99；扩展列表的编号范围为 100～199。主要的动作为允许(Permit)和拒绝(Deny)；主要的应用方法是入栈(In)应用和出栈(Out)应用。ACL 规则中包含的元素有：源 IP、目的 IP、源端口、目的端口、协议、服务等。

标准 IP ACL 主要是根据数据包源地址进行转发或阻断分组的；扩展 IP ACL 使用以上任意元素组合进行转发或阻断分组。

1. 标准 ACL

定义标准 ACL 分两步：第一步，定义规则；第二步，将规则应用在设备接口上。具体命令如下。

1)　定义规则

在路由器上使用命令：

```
Router(config)# access-list  <1-99>  { permit |deny }  源地址  [反掩码]
```

在交换机上使用命令：

```
Switch(config)# Ip  access-list  <1-99>  { permit |deny }  源地址  [反掩码]
```

2)　应用 ACL 到接口

```
Router(config-if)#ip access-group <1-99>|{name}  { in | out }
```

下面用一个例子来说明标准 ACL 的具体应用方法。如图 6.11 所示，假设要定义的规



则是只允许 172.16.3.0/24 网段访问外网 172.17.0.0/16，而禁止其他网段访问外网。

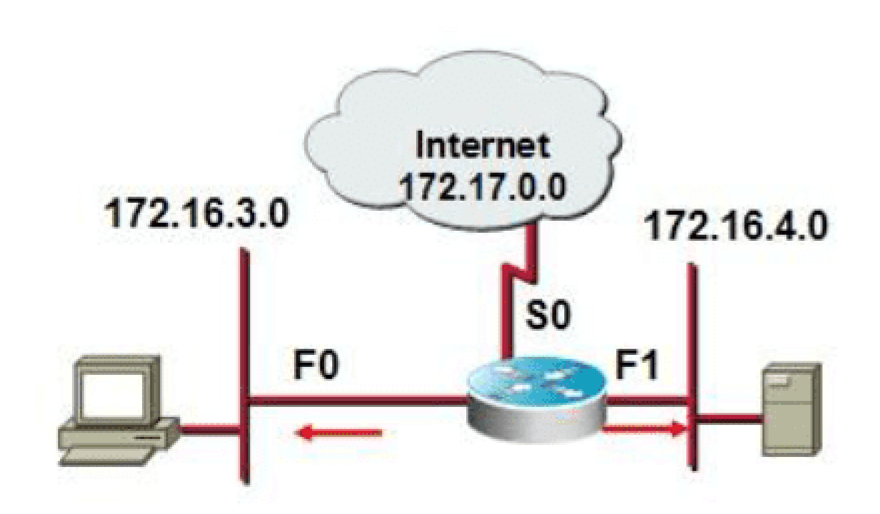


图 6.11　ACL 应用拓扑

可以在路由器上建立一个标准 ACL，编号为 1，定义以下规则：

```
Router(config)#access-list 1 permit 172.16.3.0  0.0.0.255
Router(config)#access-list 1 deny 0.0.0.0  255.255.255.255
```

然后，将上述规则应用到 S0 端口上。

```
Router(config)#interface serial S0
Router(config-if)#ip access-group 1 out
```

这里，需要注意的是，要尽量把规则应用到离限制目标最近的位置上。

2. 扩展 ACL

定义扩展 ACL 同样分两步：第一步，定义规则；第二步，将规则应用在设备接口上。不同的是限制元素得到了细化，不仅限于源 IP 地址，而且是可以根据数据包内的源、目的地址，应用服务进行过滤。

1)　定义扩展 ACL 规则

```
Router(config)# access-list <100-199> { permit /deny } 协议 源地址 反掩码 [源端口] 目的地址 反掩码 [ 目的端口 ]
```

2)　应用 ACL 到接口

```
Router(config-if)#ip access-group <100-199> |{name} { in | out }
```

在此需要注意，编号的范围为 100～199。

下面通过一个示例来说明扩展 ACL 规则定义方法：允许网络 192.168.0.0 内所有主机访问 HTTP 服务器 172.168.12.3，拒绝其他主机使用网络。

根据以上信息，可以定义以下规则：

```
Switch (config)# access-list 111  permit  tcp 192.168.0.0  0.0.255.255 host 172.168.12.3 eq www
```

上面这条规则虽然只有一条，但需注意的是，所有 ACL 默认规则是拒绝所有数据包，所以，在规则的末尾隐含一条拒绝其他主机使用网络的规则信息。

可以使用命令 Switch # show access-lists 来查看定义好的规则。

另外，不要忘了，将该规则应用到具体的某一个端口上，这一端口应尽量靠近 HTTP 服务器 172.168.12.3。

复习思考题六

一、填空题

1. 目前应用的防火墙技术主要有__________、__________、__________等。
2. 外部网络(外网)是防火墙之外的网络，一般为________，默认为________。
3. 内部网络(内网)是防火墙之内的网络，一般为________，默认为________。
4. 防火墙的分类方式有很多种。根据受保护的对象，可以分为________防火墙和防火墙；根据防火墙主要部分的形态，可以分为________防火墙和________防火墙；根据防火墙使用的对象，可以分为________防火墙和________防火墙；根据防火墙检查数据包的位置，可以分为________防火墙、________防火墙和________防火墙。
5. 目前使用的防火墙大都采用以下几种体系结构：________、________、________。
6. 防火墙的体系结构一般有__________结构、__________结构、主机过滤结构和__________结构。

二、选择题

1. 防火墙(　　)不通过它的连接。
   A. 不能控制　B. 能控制　C. 能过滤　D. 能禁止
2. 防火墙是指(　　)。
   A. 一个特定软件　B. 一个特定硬件
   C. 执行访问控制策略的一组系统　D. 一批硬件的总称
3. 包过滤防火墙工作在(　　)。
   A. 应用层　B. 会话层　C. 传输层　D. 网络层
4. 在下列防火墙体系结构中相对最安全的是(　　)。
   A. 双重宿主主机结构　B. 屏蔽主机结构　C. 屏蔽子网结构
5. 下列不属于防火墙的性能指标的是(　　)。
   A. 防火墙的并发连接数　B. 防火墙的转发速率
   C. 防火墙的延时　D. 防火墙的运行环境
6. 基于防火墙的功能分类，有__①__防火墙等；基于防火墙的工作原理分类，有__②__防火墙等。(　　) ①
   A. 包过滤、代理服务和状态检测　B. 基于路由器和基于主机系统
   C. FTP、TELNET、E-mail 和病毒　D. 双穴主机、主机过滤和子网过滤

   (　　) ②
   A. 包过滤、代理服务和状态检测　B. 基于路由器和基于主机系统
   C. FTP、TELNET、E-mail 和病毒　D. 双穴主机、主机过滤和子网过滤
7. 将防火墙软件安装在路由器上，就构成了简单的__①__；不管是哪种防火墙，都不能__②__。

   (　　) ①　A. 包过滤防火墙　B. 子网过滤防火墙
   C. 代理服务器防火墙　D. 主机过滤防火墙



(　　) ② A. 强化网络安全策略　　B. 对网络存取和访问进行监控审计

C. 防止内部信息的外泄　　D. 防范绕过它的连接

三、简答题

1. 什么是防火墙？防火墙有什么作用？
2. 防火墙有哪些优缺点？
3. 包过滤防火墙、应用代理防火墙、状态监视防火墙各有哪些优缺点？
4. 防火墙的体系结构有哪些？各有什么优缺点？
5. 防火墙的组合结构一般有哪几种形式？
6. 选择防火墙时应遵循哪些基本原则？
7. 选择防火墙时应注意哪些事项？
8. 评价防火墙性能的指标有哪些？

第 7 章　入侵检测技术

学习目标

系统学习入侵检测基本知识，入侵检测模型和体系结构及入侵检测与其他安全系统的协同。通过本章的学习，读者应掌握以下内容:

- 掌握入侵检测的概念、组成、功能及分类，入侵检测模型和体系结构。
- 了解常用的入侵检测技术，入侵检测系统与协同，入侵检测发展现状和趋势。

7.1　入侵检测概述

随着黑客入侵的日益猖獗，人们发现仅从防御的角度构造安全系统是不够的。入侵检测技术是继“防火墙”、“访问控制”等传统安全保护措施后新一代的安全保障技术。它对计算机和网络资源上的恶意使用行为进行识别和响应，它不仅检测来自外部的入侵行为，同时也监督内部用户的未授权活动。入侵检测技术是一种主动保护自己的网络和系统免遭非法攻击的网络安全技术，它从计算机系统或者网络中收集、分析信息，检测任何企图破坏计算机资源的完整性(Integrity)、机密性(Confidentiality)和可用性(Availability)的行为，即查看是否有违反安全策略的行为和遭到攻击的迹象，并做出相应的反应。

7.1.1　入侵检测概念

不同于防火墙技术，入侵检测是相对缓和的网络安全技术，这是一种被动的和事后的机制技术措施。与防火墙技术相比，虽然目前的入侵检测商业产品实用性不高，不是难以配置和维护，就是有较高的虚警率，给人的总体感觉是有负盛名，但是随着网络安全技术的发展，入侵检测系统会在整个网络安全体系中占有越来越重要的地位。作为一种积极主动的安全防护技术，入侵检测提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵。从网络安全立体纵深、多层次防御的角度出发，入侵检测理应受到人们的高度重视，这从国外入侵检测产品市场的蓬勃发展就可以看出。

James Anderson 在 20 世纪 80 年代早期首先提出了入侵检测的概念，他将入侵尝试(Intrusion Attempt)或威胁(Threat)定义为潜在的、有预谋的、未经授权的访问信息、操作信息，致使系统不可靠或无法使用的活动。

Heady 给出了另一个入侵的定义。入侵是指试图破坏资源的完整性、机密性及可用性的活动集合。

Smaha 从分类角度指出入侵包括尝试性闯入、伪装攻击、安全控制系统渗透与泄露、拒绝服务、恶意使用 5 种类型。

这里对入侵检测相关的一些基本概念作以下通俗的定义。

(1)　入侵(Intrusion)指的就是试图破坏计算机的保密性、完整性、可用性或可控性的一系列活动。



(2) 入侵活动包括非授权用户试图存取数据、处理数据，或者妨碍计算机正常运行等活动。

(3) 入侵检测(Intrusion Detection)就是对计算机网络和计算机系统的关键节点信息进行收集分析，检测其中是否有违反安全策略的事件发生或攻击迹象，并通知系统安全管理员(Site Security Officer)。

(4) 入侵检测系统(Intrusion Detection System，IDS)是用于入侵检测的软件和硬件的合称，是加载入侵检测技术的系统。

一般情况下，并不严格地去区分入侵检测和入侵检测系统两个概念，而都称为 IDS 或入侵检测技术。

7.1.2 入侵检测系统组成

入侵检测系统的基本构成如图 7.1 所示，通常由以下基本组件构成。

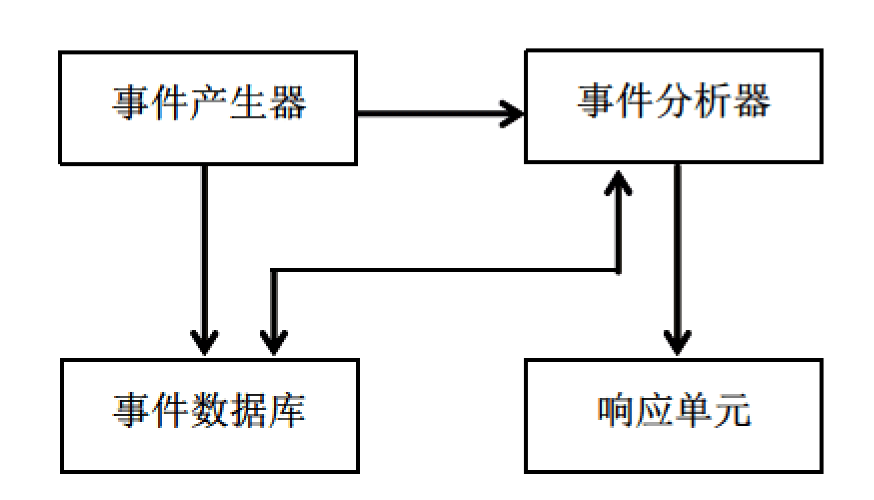


图 7.1 入侵检测系统的基本构成

(1) 事件产生器。事件产生器是入侵检测系统中负责原始数据采集的部分，它对数据流、日志文件等进行追踪，然后将搜集到的原始数据转换为事件，并向系统的其他部分提供此事件。

(2) 事件分析器。事件分析器接收事件信息，然后对它们进行分析，判断是否为入侵行为或异常现象，最后将判断的结果转变为警告信息。

(3) 事件数据库。事件数据库是存放各种中间和最终数据的地方。它从事件产生器或事件分析器接收数据，并将数据较长时间保存。事件数据库既可以是复杂的数据库，也可以是简单的文本文件。

(4) 响应单元。响应单元根据警告信息做出切断连接、改变文件属性等强烈反应，也可以只是简单的报警，是入侵检测系统中的主动武器。

以上 4 个部分只是入侵检测系统的基本组成部分。从具体实现的角度看，入侵检测系统包括硬件和软件两部分。硬件设备主要完成数据的采集和响应的实施；软件部分主要完成数据的处理、入侵的判断、响应的决策等。

基于主机的入侵检测系统相对简单；基于网络的入侵检测系统要复杂一些，一般采用分层分布式结构，主要分为数据采集层、分析层和管理层。数据采集层主要用于“抓包”，必要时做一些分包和拆包工作；分析层得到数据后对数据进行分析和判断，决定是否属于入侵行为或给出怀疑值；管理层对分析层的上报结果进行决策，做出响应，同时还担负系统维护、人机交互等任务。在网络中需要检测的点比较多，所以常采用分布式结构。



7.1.3 入侵检测功能

入侵检测系统能在入侵攻击对系统发生危害前检测到它，并利用报警与防护系统驱逐入侵攻击；在入侵攻击过程中，尽可能减少入侵攻击所造成的损失；在被入侵攻击后，能收集入侵攻击的相关信息，作为防范系统的知识添加到知识库内，从而增强系统的防范能力。

入侵检测功能可大致分为以下几个方面。

1. 监控、分析用户和系统的活动

这是入侵检测系统能够完成入侵检测任务的前提条件。入侵检测系统通过获取进出某台主机及整个网络的数据，或者通过查看主机日志等信息来监控用户和系统活动。获取网络数据的方法一般是“抓包”，即将数据流中的所有包都抓下来进行分析。

如果入侵检测系统不能实时地截获数据包并对其进行分析，就会出现漏包或网络阻塞的现象。前一种情况下系统的漏报会很多；后一种情况会影响到入侵检测系统所在主机或网络的数据流速，入侵检测系统成为整个系统的瓶颈。因此，入侵检测系统不仅要能够监控、分析用户和系统的活动，还要使这些操作足够快。

2. 发现入侵企图或异常现象

这是入侵检测系统的核心功能。主要包括两个方面：一方面是入侵检测系统对进出网络或主机的数据流进行监控，查看是否存在入侵行为；另一方面则评估系统关键资源和数据文件的完整性，查看系统是否已经遭受了入侵。前者的作用是在入侵行为发生时及时发现，从而避免系统遭受攻击；而后者一般是攻击行为已经发生，但可以通过攻击行为留下的痕迹的一些情况，从而避免再次遭受攻击。对系统资源完整性的检查也有利于对攻击者进行追踪或者取证。

对于网络数据流的监控，可以使用异常检测的方法，也可以使用误用检测的方法。目前还有很多新技术，但多数都还处在理论研究阶段。现在的入侵检测产品使用的主要还是模式匹配技术。检测技术的好坏直接关系到系统能否精确地检测出攻击，因此，对于这方面的研究是入侵检测系统研究领域的主要工作。

3. 记录、报警和响应

入侵检测系统在检测到攻击后，应该采取相应的措施来阻止或响应攻击。它应该首先记录攻击的基本情况，其次应该能够及时发出警告。良好的入侵检测系统，不仅应该能把相关数据记录在文件或数据库中，还应该提供报表打印功能。必要时，系统还能够采取必要的响应行为，如拒绝接收所有来自某台计算机的数据、追踪入侵行为等。实现与防火墙等安全部件的交互响应，也是入侵检测系统需要研究和完善的功能之一。

作为一个功能完善的入侵检测系统，除具备上述基本功能外，还应该包括其他一些功能，如审计系统的配置和弱点评估、关键系统和数据文件的完整性检查等。此外，入侵检测系统还应该为管理员和用户提供友好、易用的界面，方便管理员设置用户权限、管理数据库、手工设置和修改规则、处理报警和浏览、打印数据等。



7.2　入侵检测系统分类

根据不同的分类标准，入侵检测系统可分为不同的类别。对于入侵检测系统要考虑的因素(分类依据)主要有数据源、入侵、事件生成、事件处理及检测方法等。

7.2.1　根据数据源分类

入侵检测系统要对所监控的网络或主机的当前状态做出判断，需要以原始数据中包含的信息为基础。按照原始数据的来源，可以将入侵检测系统分为基于主机的入侵检测系统、基于网络的入侵检测系统和基于应用的入侵检测系统等类型。

1. 基于主机的入侵检测系统

基于主机的入侵检测系统主要用于保护运行关键应用的服务器，它通过监视与分析主机的审计记录和日志文件来检测入侵，日志中包含发生在系统上的不寻常活动的证据，这些证据可以指出有人正在入侵或已成功入侵了系统。通过查看日志文件，能够发现成功的入侵或入侵企图，并启动相应的应急措施。

通常情况下，基于主机的入侵检测系统可监测系统、事件、Windows NT 下的安全记录及 UNIX 环境下的系统记录，从中发现可疑行为。当有文件发生变化时，入侵检测系统将新的记录条目与攻击标记相比较，看它们是否相匹配。如果匹配，系统就会向管理员报警。对关键系统文件和可执行文件的入侵检测的一个常用方法是通过定期检查校验和来进行的，以便发现意外的变化。反应的快慢与轮询间隔的频率有直接关系。此外，许多入侵检测系统还能够监听主机端口的活动，并在特定端口被访问时向管理员报警。

2. 基于网络的入侵检测系统

基于网络的入侵检测系统主要用于实时监控网络关键路径的信息，它能够监听网络上的所有分组，并采集数据以分析可疑现象。

基于网络的入侵检测系统使用原始网络包作为数据源，通常利用一个运行在混杂模式下的网络适配器来实时监视，并分析通过网络的所有通信业务。基于网络的入侵检测系统可以提供许多基于主机的入侵检测法无法提供的功能。许多客户在最初使用入侵检测系统时，都配置了基于网络的入侵检测。

3. 基于应用的入侵检测系统

基于应用(Application)的入侵检测系统是基于主机的入侵检测系统的一个特殊子集，其特性、优缺点与基于主机的入侵检测系统基本相同。由于这种技术能够更准确地监控用户某一应用行为，所以在日益流行的电子商务中越来越受到关注。

这 3 种入侵检测系统具有互补性。基于网络的入侵检测能够客观地反映网络活动，特别是能够监视到系统审计的盲区；而基于主机和基于应用的入侵检测能够更加精确地监视系统中的各种活动。



7.2.2　根据检测原理分类

根据系统所采用的检测方法，将入侵检测分为异常入侵检测和误用入侵检测两类。

(1)　异常入侵检测。异常入侵检测是指能够根据异常行为和使用计算机资源的情况检测入侵。异常入侵检测试图用定量的方式描述可以接受的行为特征，以区分非正常的、潜在的入侵行为。Anderson 做了如何通过识别“异常”行为来检测入侵的早期工作，他提出了一个威胁模型，将威胁分为外部闯入(用户虽然被授权，但对授权数据和资源的使用不合法或滥用授权)、内部渗透和不当行为 3 种类型，并采用这种分类方法开发了一个安全监视系统，可检测用户的异常行为。

(2)　误用入侵检测。误用入侵检测是指利用已知系统和应用软件的弱点攻击模式来检测入侵。与异常入侵检测不同，误用入侵检测能直接检测不利或不可接受的行为，而异常入侵检测则是检查出与正常行为相违背的行为。

7.2.3　根据体系结构分类

按照体系结构，入侵检测系统可分为集中式、等级式和协作式 3 种。

1. 集中式

集中式入侵检测系统包含多个分布于不同主机上的审计程序，但只有一个中央入侵检测服务器，审计程序把收集到的数据发送给中央服务器进行分析处理。这种结构的入侵检测系统在可伸缩性、可配置性方面存在致命缺陷。随着网络规模的扩大，主机审计程序和服务器之间传送的数据量激增，会导致网络性能大大降低。并且一旦中央服务器出现故障，整个系统就会陷入瘫痪。此外，根据各个主机不同需求配置服务器也非常复杂。

2. 等级式

在等级式(部分分布式)入侵检测系统中，定义了若干个分等级的监控区域，每个入侵检测系统负责一个区域，每一级入侵检测系统只负责分析所监控区域，然后将当地的分析结果传送给上一级入侵检测系统。

这种结构存在以下问题：首先，当网络拓扑结构改变时，区域分析结果的汇总机制也需要做相应的调整；其次，这种结构的入侵检测系统最终还是要把收集到的结果传送到最高级的检测服务器进行全局分析，所以系统的安全性并没有实质性的改进。

3. 协作式

协作式(分布式)入侵检测系统将中央检测服务器的任务分配给多个基于主机的入侵检测系统，这些入侵检测系统不分等级，各司其职，负责监控当地主机的某些活动。所以，可伸缩性、安全性都得到了显著的提高，但维护成本也相应增大，并且增加了所监控主机的工作负荷，如通信机制、审计开销、踪迹分析等。

7.2.4　根据工作方式分类

入侵检测系统根据工作方式，可分为离线检测系统和在线检测系统。



(1) 离线检测系统。离线检测系统是一种非实时工作的系统，在事件发生后分析审计事件，从中检查入侵事件。这类系统的成本低，可以分析大量事件，调查长期的情况；但由于是在事后进行，所以不能对系统提供及时的保护，而且很多入侵在完成后都会将审计事件删除，因而无法审计。

(2) 在线检测系统。在线检测系统对网络数据包或主机的审计事件进行实时分析，可以快速响应，保护系统安全；但在系统规模较大时，难以保证实时性。

7.2.5 根据系统其他特征分类

作为一个完整的系统，其系统特征同样值得认真研究。一般来说，可以将以下一些重要特征作为分类的考虑因素。

1. 系统的设计目标

不同的入侵检测系统有不同的设计目标。有的提供记账功能，其他功能由系统操作人员完成；有的提供响应功能，根据所作出的判断自动采取相应的措施。

2. 事件生成/收集的方式

根据入侵检测系统收集事件信息的方式，可分为基于事件的和基于轮询的两类。

基于事件的方式也称为被动映射，检测器持续地监控事件流，事件的发生激活信息的收集；基于轮询的方式也称为主动映射，检测器主动查看各监控对象，以收集所需信息，并判断一些条件是否成立。

3. 检测时间(同步技术)

根据系统监控到事件和对事件进行分析处理之间的时间间隔，可分为实时和延时两类。有些系统以实时或近乎实时的方式持续地监控从信息源检测来的信息；而另一些系统在收集到信息后，要隔一定的时间后才能进行处理。

4. 入侵检测响应方式

根据入侵检测响应方式不同，可分为主动响应和被动响应。被动响应型系统只会发出告警通知，将发生的不正常情况报告给管理员，其本身并不试图降低所造成的破坏，更不会主动地对攻击者采取反击行动。

主动响应系统可以分为两类，即对被攻击系统实施控制和对攻击系统实施控制。对攻击系统实施控制比较困难，主要采用对被攻击系统实施控制，通过调整被攻击系统的状态，阻止或减轻攻击影响，如断开网络连接、增加安全日志、清除可疑进程等。

5. 数据处理地点

审计数据可以集中处理，也可以分布处理。

这些不同的分类方法可以从不同的角度了解、认识入侵检测系统，或者认识入侵检测系统所具有的不同功能。但实际的入侵检测系统常常要综合采用多种技术，具有多种功能，因此很难将一个实际的入侵检测系统归于某一类，它们通常是这些类别的混合体，某个类别只是反映了这些系统的一个侧面。

7.3　入侵检测技术

入侵检测系统常用的检测技术有误用检测、异常检测与高级检测技术。本节在介绍入侵检测技术的同时，也将对入侵响应技术进行全面分析。

7.3.1　误用检测技术

误用检测技术指通过将收集到的数据与预先确定的特征知识库里的各种攻击模式进行比较，如果发现有攻击特征，则判断有攻击，对检测已知攻击比较有效。特征知识库是将已知的攻击方法和技术的特征提取出来，来建立的一个知识库。

常用的误用检测技术有专家系统、模型推理和状态转换分析等。

1. 专家系统

专家系统是误用检测技术中运用最多的一种方法。它将有关入侵的知识转化为 If-Then 结构的规则，即将构成入侵所要求的条件转化为 If 部分，将发现入侵后采取的相应措施转化成 Then 部分。当其中某个或某部分条件满足时，系统就判断为入侵行为发生。其中的 If-Then 结构构成了描述具体攻击的规则库，状态行为及其语义环境可根据审计事件得到，推理机制根据规则和行为完成判断工作。

在具体实现中，专家系统主要面临以下问题：全面性问题，即难以科学地从各种入侵手段中抽象出全面的规则化知识；效率问题，即需要处理的数据量过大，而且在大型系统上如何获得实时、连续的审计数据也是个问题。

由于存在以上问题，商业产品一般不采用专家系统，而采用模型推理和状态转换分析方法。

2. 模型推理

模型推理是指结合攻击脚本推理出入侵行为是否出现，其中攻击行为描述攻击目的、攻击步骤以及对系统的特殊使用等。

根据这些知识建立攻击脚本库，每一脚本都由一系列攻击行为组成。检测时先将这些攻击脚本的子集看作系统正面临的攻击，然后通过一个称为预测器的程序模块根据当前行为模式，产生下一个需要验证的攻击脚本子集，并传给决策器。决策器收到信息后，根据这些假设的攻击行为在审计记录中可能出现的方式，将其翻译成与特定系统匹配的审计记录格式，最后在审计记录中寻找相应信息来确认或否认这些攻击。初始攻击脚本子集的假设应易于在审计记录中识别，且出现频率很高。随着一些脚本被确认的次数增多，另一些脚本被确认的次数减少，攻击脚本不断得到更新。

模型推理方法的优点是对不确定性的推理有合理的数学理论基础，同时决策器使得攻击脚本可以与审计记录的上下文无关。此外，这种检测方法也减少了需要处理的数据量，因为它首先按脚本类型检测相应类型是否出现，然后再检测具体的事件。其缺点在于创建入侵检测模型的工作量比别的方法要大，在系统实现时，决策器如何有效地翻译攻击脚本也是一个问题。



3. 状态转换分析

状态转换分析最早是由 R.Kemmerer 提出的，即将状态转换图应用于入侵行为的分析。

状态转换法将入侵过程看作一个行为序列，这个行为序列导致系统从初始状态转入被入侵状态。分析时，首先针对每一种入侵方法确定系统的初始状态和被入侵状态以及导致状态转换的条件，即导致系统进入被入侵状态必须执行的操作(特征事件)。然后用状态转换图来表示每一个状态和特征事件，这些事件被集成于模型中，所以检测时不需要逐条查找审计记录。但是，状态转换是针对事件序列进行的分析，所以不善于分析过于复杂的事件，而且不能检测与系统状态无关的入侵。

同专家系统一样，对事件序列分析也需要知道攻击行为的具体知识。但是，攻击方法的语义描述不是被转化为检测规则，而是在审计记录中能直接找到的信息形式。这样就不像专家系统一样需要处理大量数据，从而大大提高了检测效率。这种方法的缺陷也和所有其他的误用检测方法一样，需要经常为新发现的系统漏洞更新知识库；另外，由于对不同操作系统平台的具体攻击方法不同，以及不同平台的审计方式不同，所以构造和维护的工作量都较大。

Petri 网就是一种类似于状态转换图分析的方法。它能一般化、图形化地表达状态，并且简洁、明了。虽然复杂的入侵特征能用 Petri 网表达得很简单，但是对原始数据匹配时的计算量却很大。

7.3.2　异常检测技术

误用检测技术需要已知入侵的行为模式，所以不能检测未知的入侵。异常检测则可以检测未知的入侵。基于异常检测的入侵检测首先要构建用户正常行为的统计模型，然后将当前行为与正常行为特征相比较来检测入侵。常用的异常检测技术有概率统计方法和神经网络方法两种。

1. 概率统计方法

概率统计方法是异常检测技术中应用最早也是最广泛的一种方法。首先，检测器根据用户的动作建立用户特征表，通过比较当前特征与已存储定型的特征，从而判断是否为异常行为。用户特征表需要根据审计记录情况不断加以更新。

用于描述特征的变量类型有以下几种。

(1)　操作密度。度量操作执行的频率，常用于检测一段时间内的异常行为。

(2)　审计记录分布。度量在最新记录中所有操作类型的分布情况。

(3)　范畴尺度。度量在一定动作范畴内特定操作的分布情况。

(4)　数值尺度。度量产生数值结果的操作，如 CPU 占用率、I/O 使用频繁程度等。

这些变量所记录的具体操作包括 CPU 的使用、I/O 的使用、使用地点及时间、邮件使用、编辑器使用、编译器使用以及所创建、删除、访问或改变的目录及文件、网络活动等。

在入侵检测研究机构 SRI/CSL(Stanford Research Institute/Computer Science Laboratory)的入侵检测专家系统中给出了一个特征简表的结构：

<变量名，行为描述，例外情况，资源使用，时间周期，变量类型，阀值，主体，客体，值>

其中的变量名、主体、客体唯一确定每一个特征简表，特征值由系统根据审计数据周期性地产生。这个特征值是所有用户特征异常程度值的函数。如果假设 S_1，S_2，…，S_n 分别是用于描述特征的变量 M_1，M_2，…，M_n 的异常程度值，$S_i(i=1, 2, \cdots, n)$值越大，说明异常程度越大。这个特征值可以用所有 S_i 值的加权平方和来表示：

$$M=a_1S_1^2+a_2S_2^2+\cdots+a_nS_n^2,\quad a_i>0(i=1, 2, \cdots, n)$$

式中，a_i 为每一种特征的权重。

如果选用标准偏差作为判别准则，则标准偏差计算公式如下：

$$\sigma=\sqrt{M/(n-1)-\upsilon^2}$$

其中，

$$\upsilon=M/n$$

如果某异常程度值 S 超出了 $\upsilon\pm\sigma$，就认为出现异常。

概率统计方法的优越性在于能应用成熟的概率统计理论。但也有一些不足之处，如统计检测对事件发生的次序不敏感，也就是说，完全依靠统计理论可能漏检那些利用彼此关联事件的入侵行为。其次，定义是否入侵的异常程度值 S 也比较困难。S 太低，则漏检率提高；S 太高，则误检率提高。

2. 神经网络方法

利用神经网络检测入侵的基本思想是用一系列信息单元(命令)训练神经元，这样在给定一组输入值后，就可能预测出输出结果。与统计理论相比，神经网络更好地表达了变量间的非线性关系，并且能自动学习和更新。实验表明，UNIX 系统管理员的行为几乎全是可以预测的，不可预测的行为只占了很少的一部分。

神经网络模块结构是当前命令和刚过去的 N 个命令组成了神经网络的输入层，其中 N 是神经网络预测下一个命令时所包含的过去命令集的大小。根据用户的典型命令序列训练网络后，该网络就形成了对应用户的特征命令表，网络对当前用户事件与用户的特征命令表中的事件进行比较，预测用户行为是否异常。基于神经网络的检测思想示意图如图 7.2 所示。

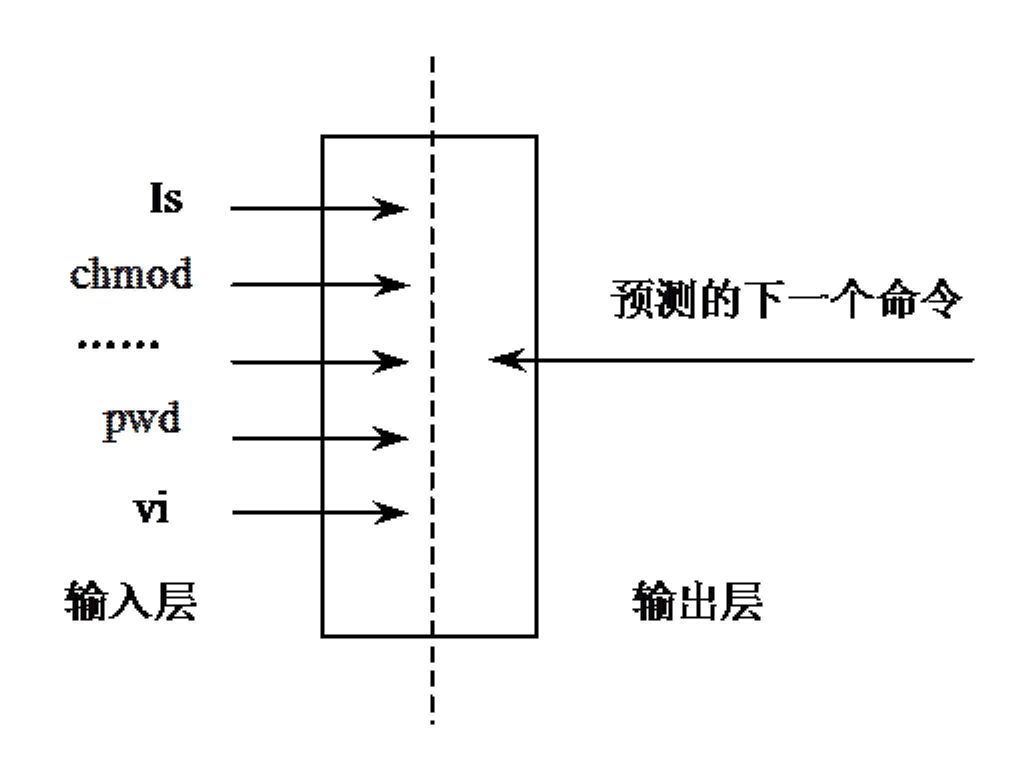


图 7.2　用于入侵检测的神经网络示意图

图 7.2 中，输入层的 N 个箭头代表了用户最近的 N 个命令，输出层预测用户将要发生的下一个动作。神经网络方法的优点在于能更好地处理原始数据的随机特征，即不需要对这些数据做任何统计假设，并且有较好的抗干扰能力。缺点在于网络拓扑结构以及各元素



的权重很难确定，命令窗口 N 的大小也难以选取。窗口太小，则网络输出不好；窗口太大，则网络会因为处理大量无关数据而降低效率。

7.3.3 高级检测技术

高级检测技术主要包括文件完整性检查、计算机免疫技术、遗传算法、模糊证据理论、数据挖掘和数据融合等。

1. 文件完整性检查

文件完整性检查系统检查计算机中自上次检查后文件的变化情况，它能够保存每个文件的数字文摘数据库，每次检查时，重新计算文件的数字文摘，并将其与数据库中的值相比较。如不同则说明文件已被修改；若相同，则说明文件未发生变化。

文件的数字文摘通过 Hash 函数计算得到。不管文件长度如何，其计算结果都是一个固定长度的数字。与加密算法不同，Hash 算法是一个不可逆的单向函数。采用安全性高的 Hash 算法，如 MD5、SHA 时，两个不同的文件几乎不可能得到相同的 Hash 结果。因此，文件一旦被修改，就可检测出来。

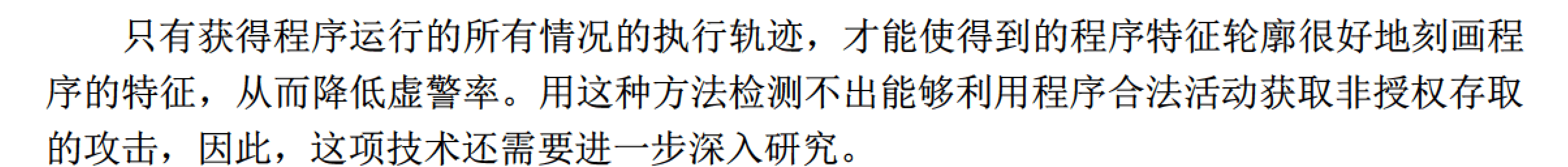
在文件完整性检查中功能最全面的当数 Tripwire，其开放源代码的版本可以从 Http://www.tripwire.org 中获得。文件完整性检查系统具有以下优点：从数学上分析，攻克文件完整性检查系统，无论是时间上还是空间上都是不可能的。文件完整性检查系统具有相当大的灵活性，可以配置成监测系统中的所有文件或某些重要文件。当一个入侵者攻击系统时，首先，他要通过更改系统中的可执行文件、库文件或日志文件来隐藏他的活动；其次，他要做一些改动以保证下次能够继续入侵。这两种活动都能够被文件完整性检查系统检测出来。

文件完整性检查系统的弱点是依赖于本地的文摘数据库。与日志文件一样，这些数据可能被入侵者修改。当一个入侵者取得管理员权限，在完成破坏活动后，可以运行文件完整性检查系统更新数据库，从而瞒过系统管理员。做一次完整的文件完整性检查非常耗时。在 Tripwire 中，可选择检查某些系统特性而不是完全的摘要，从而加快检查速度。系统有些正常的更新操作可能会带来大量的文件更新，从而增加比较繁杂的检查与分析工作，如在 Windows NT 系统中升级 Outlook 将会带来 1800 多个文件变化等。

2. 计算机免疫技术

Forrest 等首次提出计算机免疫技术，这种免疫机制在处理外来异常时呈现了分布的、多样性的、自治的及自修复的特征，免疫系统通过识别异常或以前未出现的特征来确定入侵。计算机免疫技术为入侵检测提供了一个思路，即通过正常行为的学习来识别不符合常态的行为序列。

当系统的一个关键程序投入使用后，其与系统用户行为的易变性相比，具有相对的稳定性。因而可以利用系统进程正常执行轨迹中的系统调用序列集，来构建系统进程正常执行活动的特征轮廓。由于利用这些关键程序的缺陷进行攻击时，对应的进程必然执行一些不同于正常执行时的代码分支，因而就会出现关键程序特征轮廓中没有的系统调用序列。当检测到该调用序列的量达到某一条件后，就认为被监控的进程企图攻击系统。



只有获得程序运行的所有情况的执行轨迹，才能使得到的程序特征轮廓很好地刻画程序的特征，从而降低虚警率。用这种方法检测不出能够利用程序合法活动获取非授权存取的攻击，因此，这项技术还需要进一步深入研究。

3. 遗传算法

遗传算法的基本思想来源于 Darwin 的进化论和 Mendel 的遗传学说，最早由 BagleyJ.D 在 1967 年提出。遗传算法在入侵检测中的应用时间不长，在一些研究试验中，利用若干字符串序列来定义用于分析检测的指令组，这些指令在初始训练阶段不断进化，提高了分析能力。此外，也有人将遗传算法与神经网络相结合，将其应用于网络的学习、网络的结构设计和网络的分析等方面，然后应用到入侵检测领域。

遗传算法虽然潜力巨大、前景广阔，但其本身还有很多问题有待探讨，应用还有待于进一步的研究。

4. 模糊证据理论

入侵检测的评判标准本身就具有一定的模糊性，模糊证据理论因此被引入到入侵检测中。李之棠等建立了一种基于模糊专家系统的入侵检测框架模型，该模型吸收了误用检测和异常检测的优点，能较好地降低漏警率和虚警率。

5. 数据挖掘

数据挖掘(Data Mining)也称数据库中的知识发现(Knowledge Discovery in Database，KDD)。数据挖掘是指从大型数据库中提取人们感兴趣的知识，提取的知识一般可表示为概念(Concepts)、规则(Rules)、规律(Regularities)和模式(Patterns)等形式。数据挖掘是一门交叉性学科，涉及机器学习、模式识别、归纳推理、统计学、数据库、数据可视化及高性能计算等多个领域。

数据挖掘技术在入侵检测中主要有两个方向：一是发现入侵的规则、模式，与模式匹配检测方法相结合；二是用于异常检测，找出用户正常行为，创建用户的正常行为库。提出这个技术的目的之一是为了弥补模式匹配技术对未知攻击无能为力的弱点；还有就是使检测模型的构建自动化，发展异常检测方法。

6. 数据融合

数据融合是针对同一系统中使用多个或多类传感器这一特定问题展开的一种新的数据处理方法，因此数据融合又称为多传感器信息融合或信息融合。多传感器数据融合的定义可概括为充分利用不同时间与空间的多传感器数据资源，采用计算机技术对按时间序列获得的多传感器观测数据，在一定规则下进行分析、综合、支配和使用，获得对被测对象的一致性解释与描述，进而实现相应的决策和评估，使系统获得比其各组成部分更充分的信息。

多传感器系统是数据融合的硬件基础，多源信息是数据融合的加工对象，协调优化和综合处理是数据融合的核心。

数据融合系统主要有局部式和全局式两种。局部式又称为自备式，这种数据融合系统收集来自单个平台的多个传感器数据，也可以用于检测对象相对单一的智能检测系统中。



全局式又称为区域式，这种数据融合系统组合来自空间和时间上各不相同的多平台、多个传感器的数据，大型军事防御系统与多参数或参数间交叉影响的智能检测系统大都采用这种融合方式。

多传感器数据融合与单传感器处理相比，其复杂性大大增加。

数据融合的入侵检测系统要能够提供高质量的信息，即提供的信息要比没有采用融合的系统提供的信息具有更高的质量。因此能降低系统的误报数量和误警率。

7.3.4 入侵诱骗技术

1. 概念

入侵诱骗技术是较传统入侵检测技术更为主动的一种安全技术。入侵诱骗技术包括蜜罐(Honeypot)和蜜网(Honeynet)两种，加载蜜罐技术和蜜网技术的系统分别称为蜜罐系统和蜜网系统。顾名思义，入侵诱骗技术就是用特有的特征吸引攻击者，以便对攻击者的各种攻击行为进行分析，并找到有效的对付方法。为了吸引攻击者，网络安全专家通常还在蜜罐上故意留下一些安全后门，或者放置一些网络攻击者希望得到的敏感信息(当然这些信息都是虚假的信息)。当攻击者正为攻入目标系统而沾沾自喜，他在目标系统中的所有行为，包括输入的字符、执行的操作等都已经被蜜罐所记录。

2. 蜜罐技术

蜜罐是一种被侦听、被攻击或已经被入侵的资源，也就是说，无论如何对蜜罐进行配置，最终目的就是使得整个系统处于被侦听、被攻击的状态。蜜罐并非一种安全解决方案，这是因为它并不会“修理”任何错误，它只是一种工具，如何使用这个工具取决于使用者想要做什么。

蜜罐可以仅仅是一个对其他系统和应用的仿真，也可以创建一个监禁环境将攻击者围困其中，还可以是一个标准的产品系统。无论使用者如何建立和使用蜜罐，只有蜜罐受到攻击，其作用才能发挥出来。

为了方便攻击者攻击，最好是将蜜罐设置成域名服务器(Domain Name Server，DNS)、Web 或电子邮件转发服务等流行应用中的某一种。

从传统意义上讲，网络安全要做的工作主要是防御，防止自己负责的资源免受入侵者攻击；尽力保护自己的系统，检测防御中的失误，并采取相应的措施，这些安全措施都只能检测到已知类型的攻击和入侵。而蜜网设计的目的就是从现存的各种威胁中提取有用的信息，发现新型的攻击工具，确定攻击的模式并研究攻击者的攻击动机。

3. 蜜网技术

蜜网可以获取攻击者信息，大部分传统的蜜罐都进行对攻击的诱骗或检测。这些传统的蜜罐通常都是一个单独的系统，用于模拟其他系统、已知的服务和弱点。蜜网不同于传统的蜜罐，它并不是一种比传统的蜜罐更好的解决方案，只是其侧重点不同而已。其工作实质是在各种网络迹象中获取所需的信息，而不是对攻击进行诱骗或检测。

蜜网在设计上与蜜罐有两点不同。

(1) 蜜网不是一个单独的系统，而是由多个系统和多个攻击检测应用组成的网络。这

个网络放置在防火墙后，可以监控、捕获并控制所有进出网络的数据，根据捕获的数据信息分析的结果就可以得到攻击组织所使用的工具、策略和动机。

蜜网内可以同时包含多种系统，比如 Solaris、Linux、Windows NT、Cisco 路由器和 Alteon 交换机等，可以创建一个反映真实产品情况的网络环境。此外，不同的系统还可以采用不同的应用，比如 Linux DNS 服务器、Windows IIS 网络服务器和 Solaris 数据库服务器等，这样就可以更加准确地概括不同攻击者的不同意图和特点。

(2) 所有放置在蜜网中的系统都是标准的产品系统。这些系统和应用都是用户可以在 Internet 上找到的真实系统和应用。该网络中的任何一部分都不是模拟的应用，并且这些应用都具有与真实的系统相同的安全等级。因此，在蜜网中发现的漏洞和弱点就是真实存在并需要改进的问题，用户所需做的就是将系统从产品环境移植到蜜网中。

7.3.5 入侵响应技术

入侵响应技术是入侵检测技术的配套技术，一般的入侵检测系统会同时使用这两种技术。根据系统设计的功能和目的不同，有时也称以实施入侵响应技术为主的系统为入侵响应系统。

入侵响应技术可分为主动响应和被动响应两种类型。在主动响应里，入侵检测系统能阻塞攻击，或影响进而改变攻击的进程；在被动响应里，入侵检测系统仅仅简单地报告和记录所检测出的问题。主动响应和被动响应并不是相互排斥的。不管使用哪一种响应机制，入侵检测系统总能以日志的形式记录检测结果。

1. 主动响应

主动响应即检测到入侵后立即采取行动。主动响应有两种形式：一种是由用户驱动的，另一种是由系统本身自动执行的。对入侵者采取反击行动，修正系统环境和收集尽可能多的信息是主动响应的基本手段。

1) 对入侵者采取反击行动

警告攻击者、跟踪攻击者、断开危险连接和对攻击者的攻击是最严厉的一种主动反击手段。这种响应方法有一定的风险。

(1) 根据黑客最常用的攻击方法，被确认为攻击的源头系统很可能是黑客的另一个牺牲品。成功攻击一个系统，然后使用他作为攻击另一个系统的平台，这是攻击者进行攻击的基本手段之一。如果瞄准这个攻击源头系统，很可能反击的是一个无辜的同伴。

(2) 即使攻击者确实来自一个合法控制的系统，但如果使用攻击源 IP 地址欺骗，攻击系统的源 IP 地址实际上可能是另一个牺牲者。

(3) 简单的反击可能会惹起对手更大的攻击。

(4) 在许多情况下，反击会冒违法犯罪的风险。如果你的行为攻击了无辜的一方，该方可能要控告你，并要求赔偿其损失。况且，你的反击本身可能违反了计算机相关法规。

对入侵者采取反击行动也可以以温和的方式进行。比如，记录安全事件、产生报警信息、记录附加日志和激活附加入侵检测工具等。

介于温和与严厉之间的手段有隔离入侵者 IP、禁止被攻击对象的特定端口和服务以及隔离被攻击对象等。



另一种响应方式是自动地向入侵者可能来自的系统的管理员发送 E-mail，并且请求协助确认入侵者和处理相关问题。当黑客通过拨号连接进入系统时，这种响应方式还能产生多种用途。

2) 修正系统环境

修正系统环境较直接采取反击的主动性要差一些，当与提供调查支持的响应结合在一起时，却往往是一种更好的响应方案。在一些入侵检测系统中，这类响应也许通过增加敏感程度改变分析引擎的操作特征，通过插入规则改变专家系统，即通过这些规则提高对某些攻击的怀疑水平，或增加监视范围以更好地收集信息。这种策略类似于实时过程控制系统中的反馈机制，即目前系统处理过程的输出将用来调整和优化下一个处理过程。

3) 收集额外信息

主动响应的第 3 种方法是收集额外信息。当被保护的系统非常重要且系统的主人想进行配置改进时，这种方法特别有用。前面提到的蜜罐技术实际上就是一种有效的收集信息的手段，以这种方式收集的信息对那些网络安全威胁趋势分析人员来说也是有价值的。

2. 被动响应

被动响应就是只向用户提供信息，而由用户去决定是否采取下一步行动的响应。在早期的入侵检测系统里，所有的响应都是被动的。以下列举两种常用的被动响应技术。

1) 告警和通知

绝大多数入侵检测系统提供多种形式的告警生成方式以供选择，允许用户设置告警以适合本组织的系统操作程序规范。

(1) 告警显示屏。入侵检测系统提供的最常用的告警和通知方式是屏幕告警或窗口告警，这种告警消息出现在入侵检测系统控制台上，或由用户配置的其他系统上。在告警消息方面，不同的系统提供不同的详细程度，范围从简单的“一个入侵已经发生”到列出此问题的表面源头、攻击的目标、入侵的本质意图以及攻击是否成功等广泛性记录。在一些系统里告警消息的内容也可以用户自己定制。

(2) 告警和警报的远程通知。按时钟协调运行多系统的组织使用另一种告警/警报形式。在这些情形下，入侵检测系统能通过拨号或移动电话向系统管理员或安全工作人员发出告警和警报消息。

E-mail 消息是另一种通知手段，在某些情形下，通知选项允许用户配置附加信息或告警编码给相应单位。

2) SNMP 陷阱和插件

Internet 上的 SNMP 陷阱服务接收由本地或远程 SNMP 代理生成的陷阱消息，然后将这些消息转发给用户的计算机上运行的 SNMP 管理程序。为代理配置了 SNMP 陷阱服务后，如果发生任何特定的事件，都将生成陷阱消息。这些消息被发送到陷阱目标。例如，可以将代理配置为在无法识别的管理系统发送信息请求时启动身份验证陷阱。陷阱目标包括管理系统的计算机名、IP 地址或 Internet 数据包交换(IPX)地址。陷阱目标必须是启用网络并且运行 SNMP 管理软件的主机。

有些入侵检测系统与网络管理工具一起使用。它能使用网络管理基础设施来传送在网络管理控制台显示的告警和警报信息，它依附简单网络管理协议(SNMP)的消息或陷阱作为

一个告警选项。一些商业化产品里提供这个功能选项，入侵检测系统有可能和网络管理系统更彻底地集成在一起。这种集成能提高使用通信信道的能力和网络环境中对安全提供主动响应的能力。

7.4　入侵检测体系

本节在给出通用入侵检测模型的基础上，对主机入侵检测系统、网络入侵检测系统和分布式入侵检测系统的概念和特点进行集中讲解。

7.4.1　入侵检测模型

为了更好地研究入侵检测系统，人们将其各个组成部分抽象出来，形成各种入侵检测模型。较通用的模型有 Denning 模型和 CIDF 模型。

1. Denning 模型

Denning 于 1987 年提出了一个通用的入侵检测模型，如图 7.3 所示。

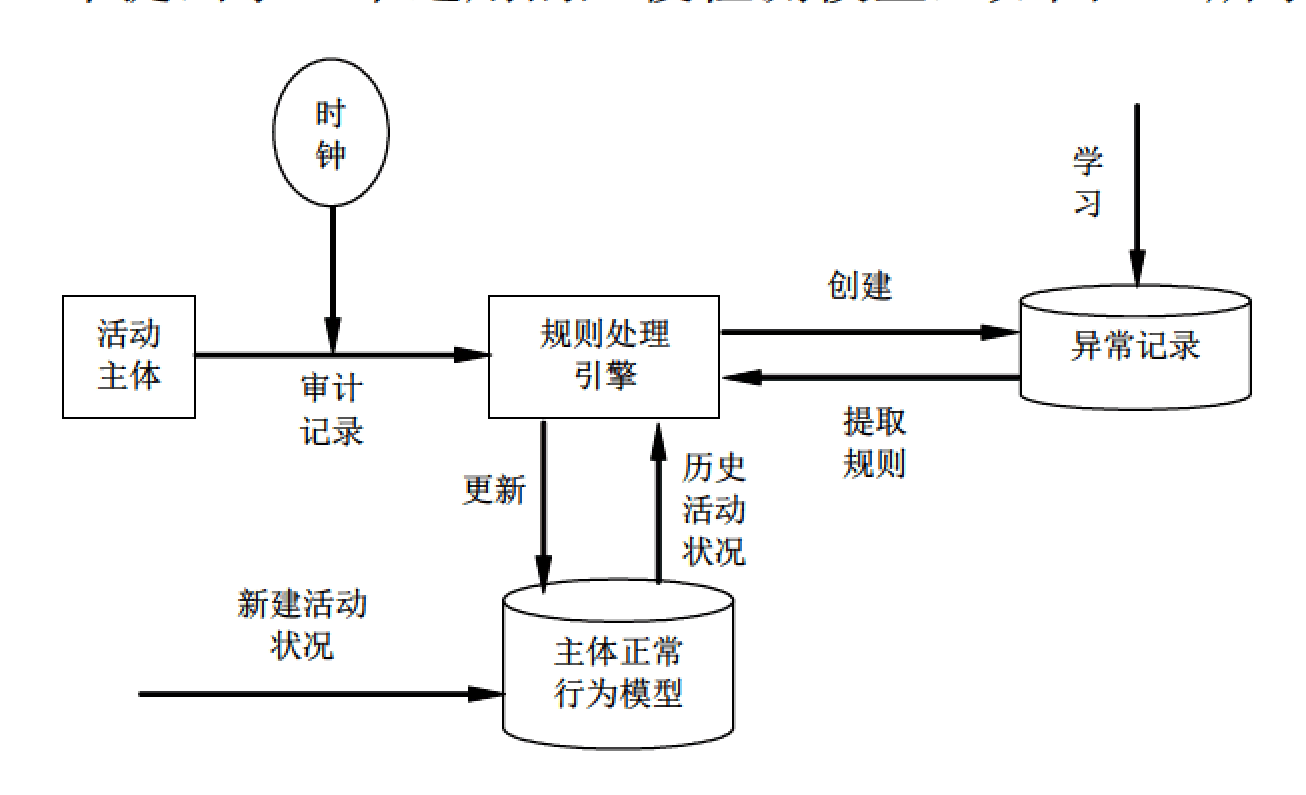


图 7.3　Denning 入侵检测模型

图 7.3 所示的模型中包含 6 个主要部分。

(1)　主体(Subjects)。在目标系统上活动的实体，如用户。

(2)　对象(Objects)。指系统资源，如文件、设备、命令等。

(3)　审计记录(Audit Records)。由主体、活动(Action)、异常条件(Exception-Condition)、资源使用状况(Resource-Usage)和时间戳(Time-Stamp)等组成。其中活动是指主体对目标的操作，异常条件是指系统对主体的异常情况的报告，资源使用状况是指系统的资源消耗情况。

(4)　活动档案(Active Profile)。即系统正常行为模型，保存系统正常活动的有关信息。在各种检测方法中其实现各不相同。在统计方法中可以从事件数量、频度、资源消耗等方面度量。

(5)　异常记录(Anomaly Record)。其由事件、时间戳和审计记录组成，表示异常事件的发生情况。

(6)　活动规则(Active Rule)。判断是否为入侵的准则及要采取的行动。一般以系统正常活动模型为基准，根据专家系统或统计方法对审计记录进行分析处理，在发现入侵时采取



相应的对策。

2. CIDF 模型

CIDF(Common Intruction Detection Framework，入侵检测系统的通用模型)包括入侵检测系统的体系结构、通信机制、描述语言和应用编程接口(API)等 4 个方面。

其中体系结构如图 7.4 所示。模型中，入侵检测系统分为 4 个基本组件，即事件产生器、事件分析器、响应单元和事件数据库。其中的事件是指入侵检测系统需要分析的数据。这 4 个组件只是逻辑实体，一个组件可能是某台计算机上的一个进程甚至线程，也可能是多个计算机上的多个进程。它们以 GIDO(统一入侵检测对象)格式进行数据交换。

这种划分体现了入侵检测系统所必须具有的体系结构：数据获取、数据分析、行为响应和数据管理，因此具有通用性。事件产生器、事件分析器和响应单元通常以应用程序的形式出现，而事件数据库则以文件或数据流的形式出现。GIDO 数据流可以是发生在系统中的审计事件或对审计事件的分析结果。

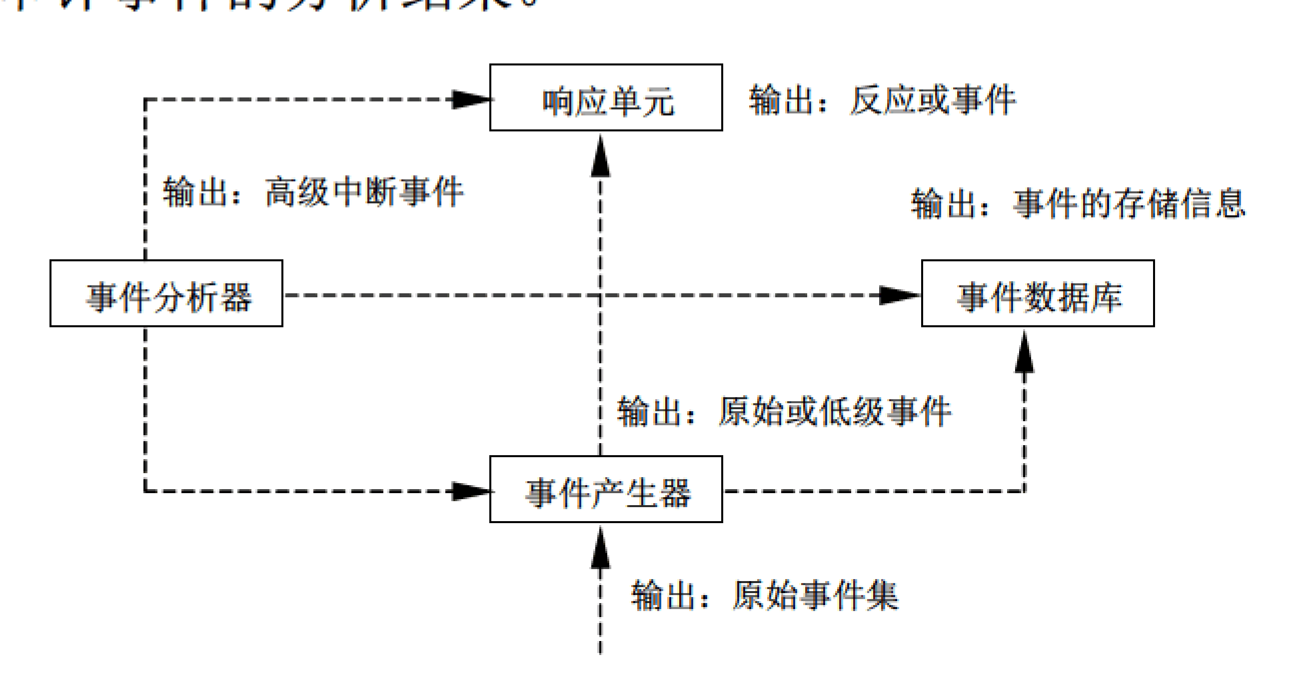


图 7.4　CIDF 入侵检测模型

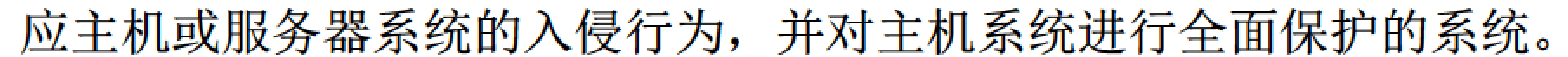
事件产生器的任务是从入侵检测系统之外的计算机中收集事件，但不作分析，将这些事件转换成 CIDF 的 GIDO 格式传送给其他组件；事件分析器分析收到的 GIDO，并将产生的新的 GIDO 再传送给其他组件；事件数据库用来存储 GIDO，以备系统使用；响应单元处理收到的 GIDO，并根据处理结果采取相应的措施，如删除相关进程、将连接复位及修改文件权限等。

7.4.2　入侵检测体系结构

根据入侵检测系统的保护对象或数据来源，可以将入侵检测技术分为主机入侵检测技术和网络入侵检测技术两种。作为这两类技术的实施体系，主机入侵检测系统和网络入侵检测系统是两类基本的入侵检测体系，混合入侵检测系统和分布式入侵检测系统则是在此基础上的延伸。

1. 主机入侵检测

基于主机的入侵检测出现在 20 世纪 80 年代初期，那时网络还没有像今天这样普及、复杂，且网络之间也没有完全连通。在这较为简单的环境里，检查可疑行为的检验记录是很常见的操作。由于入侵在当时是相当少见的，因此对攻击进行事后分析就可以防止以后的攻击。主机入侵检测系统确切的定义就是，安装在单个主机或服务器系统上，监测和响



应主机或服务器系统的入侵行为，并对主机系统进行全面保护的系统。

主机入侵检测系统主要是对该主机的网络连接行为，以及系统审计日志进行智能分析和判断。如果其中主体活动十分可疑，入侵检测系统就会采取相应措施。作为对主机系统的全面防护，主机入侵检测通常包括网络监控和主机监控两个方面。

主机入侵检测系统在发展过程中融入了其他技术，是对关键系统文件和可执行文件的入侵检测的一个常用方法，是通过定期检测和校验进行的，以便发现意外的变化。反应的快慢与轮询的频率有直接的关系。最后，许多产品都是监听端口的活动，并在特定端口被访问时向管理员报警。这类检测方法将基于网络的入侵检测的基本方法融入到基于主机的检测环境中。尽管后者不如前者快捷，但却有前者无法比拟的优点。

(1) 性能价格比高。在主机数量较少的情况下，这种方法的性能价格比较高。尽管基于网络的入侵检测系统能很容易地提供广泛覆盖，但其价格通常很高，而基于主机的入侵检测系统花销较小，客户只需很少的费用用于最初的安装。

(2) 细致性。基于主机的入侵检测系统能够监视用户和文件访问活动，包括文件访问、改变文件权限、试图建立新的可执行文件及试图访问特许服务等。例如，基于主机的入侵检测系统可以监督所有用户登录及退出登录的情况，以及每个用户在连接到网络以后的行为。此外，基于主机技术还可监视通常只有管理员才能实施的非正常行为，并且能够记录所有用户账号的添加、删除、更改的情况。

(3) 针对性。一旦入侵者得到了一个主机的用户名和口令，基于主机的入侵监测系统最有可能区分正常的活动和非法的活动。

(4) 易于删除。每一个主机有自己的代理，用户删除更方便。

(5) 无须专门硬件。基于主机的方法有时不需要增加专门的硬件平台。基于主机的入侵检测系统存在于现有的网络结构中，包括文件服务器、Web 服务器及其他共享资源，因此，基于主机的系统效率很高。

(6) 对网络流量不敏感。用代理的方式一般不会因为网络流量的增加而放弃对网络行为的监视。

(7) 适用于被加密的及切换的环境。由于基于主机的系统安装在遍布企业的各种主机上，因此它们有比基于网络的入侵检测系统更加加密的环境。交换设备可将大型网络分成许多小型网络段加以管理，所以从覆盖足够大的网络范围的角度出发，很难确定配置基于网络的入侵检测系统的最佳位置。基于主机的入侵检测系统可安装在所需的重要主机上，在交换的环境中具有更高的能见度。

根据加密方式在协议堆栈中位置的不同，基于网络的系统可能对某些攻击没有反应。对基于主机的入侵检测系统没有这方面的限制。

(8) 确定攻击是否成功。由于基于主机的入侵检测系统使用已发生事件的信息，因此它比基于网络的入侵检测系统更能准确地判断攻击是否成功。

2. 网络入侵检测

网络入侵检测使用原始网络包作为数据源，它通常利用一个运行在混杂模式下的网络适配器来实时监视并分析通过网络的所有通信业务，其攻击识别模块通常使用 4 种常用技术来识别攻击标志，即模式、表达式或字节匹配、频率或穿越阈值、次要事件的相关性和



非常规现象检测等。

一旦检测到攻击行为，入侵检测系统的响应模块就提供多种选项以通知、报警，并对攻击采取相应的反应。反应因产品而异，但通常都包括通知管理员、中断连接并且做会话记录等。实际上，许多客户在最初使用入侵检测系统时，都配置了基于网络的入侵检测。

基于网络的入侵检测系统有以下优点。

(1) 检测速度快。基于网络的监测器通常能在μs 或 s 级时间内发现问题，而大多数基于主机的产品则要依靠对最近几分钟内审计记录的分析才能得出结果。

(2) 隐蔽性好。网络上的监测器不像主机那样显眼和易被存取，因而也不容易遭受攻击。基于网络的监视器不运行其他应用程序，不提供网络服务，可以不响应其他计算机，因此比较安全。

(3) 视野更宽。基于网络的入侵检测可以在网络的边缘上(即攻击者还没能接入网络时)就被发现并被制止。

(4) 较少的监测器。由于使用一个监测器就可以保护一个共享的网段，所以不需要很多的监测器；相反，如果基于主机，则在每个主机上都需要一个代理，成本很高且难以管理。

(5) 攻击者不易转移证据。基于网络的入侵检测系统使用正在发生的网络通信进行实时攻击的检测，所以攻击者无法转移证据。被捕获的数据不仅包括攻击的方法，而且还包括可识别黑客身份和对其进行起诉的信息。许多黑客都熟知审计记录，他们知道如何操纵这些文件来掩盖作案痕迹。

(6) 操作系统无关性。基于网络的入侵检测系统作为安全监测资源，与主机的操作系统无关。与之相比，基于主机的系统必须在特定的、没有遭到破坏的操作系统中才能正常工作。

(7) 占用资源少。在被保护的设备上不必占用任何资源。

网络入侵检测系统存在以下弱点。

(1) 网络入侵检测系统只检测直接连接到的网段通信，不能检测不同网段的网络数据包。

(2) 在使用交换以太网的环境中会出现检测范围受限。

(3) 安装多台网络入侵检测系统的传感器会使部署整个系统的成本大大增加。

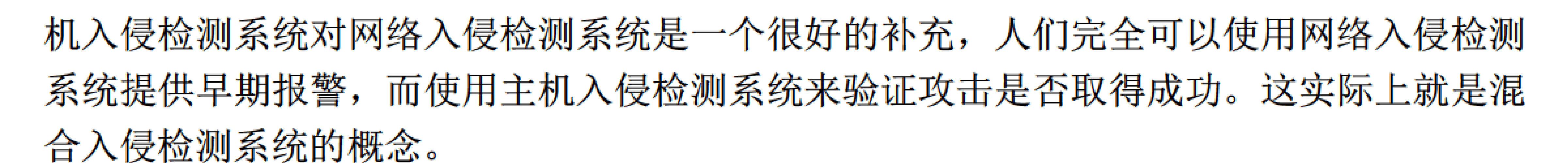
(4) 网络入侵检测系统为了优化性能通常采用特征检测的方法，可以检测出普通的攻击，但很难实现一些复杂的、需要大量计算与分析时间的攻击检测。

(5) 网络入侵检测系统会将大量的数据传回分析系统中，在监听特定的数据包时会产生大量的分析数据流量。因而传感器协同工作能力较弱。

(6) 网络入侵检测系统处理加密的会话过程比较困难，目前，通过加密通道的攻击尚不多，但随着 IPv6 的普及，这个问题会越来越突出。

3. 混合入侵检测

主机入侵检测系统和网络入侵检测系统各有其优缺点，混合使用基于主机和基于网络这两种方式能够达到更好的检测效果。例如，主机入侵检测系统使用系统日志作为检测依据，在确定攻击是否已经取得成功时与网络入侵检测系统相比具有更大的准确性，因此主



机入侵检测系统对网络入侵检测系统是一个很好的补充，人们完全可以使用网络入侵检测系统提供早期报警，而使用主机入侵检测系统来验证攻击是否取得成功。这实际上就是混合入侵检测系统的概念。

4. 分布式入侵检测

分布式入侵检测系统可以是混合入侵检测系统的一种，也可以仅仅是网络入侵检测系统的分布式整合。

传统的集中式入侵检测技术的基本原理是在网络的不同网段中放置多个传感器或探测器，首先收集当前网络状态的信息，然后将这些信息传送到中央控制台进行处理和分析。更进一步，有的传感器具有某种主动性，能够接收中央控制台的某些命令和下载某些识别模板。

集中式模型具有以下几个明显的缺陷。

(1) 面对在大规模、异构网络基础上发起的复杂攻击行为，会增加中央控制台的工作负荷，以至于它无法具有足够的能力处理来自四面八方的消息事件。因此，会遗漏许多重大消息事件，从而增加漏警率。

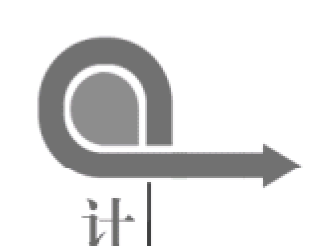
(2) 由于网络传输的延时问题，到达中央控制台的数据包中的事件消息只是反映了其刚被生成时的情况，而不能反映随着时间而改变的当前状态。这使得基于过时信息做出的判断的可信度大大降低，同时也使得确认相关信息的来源变得非常困难。

(3) 异构网络环境所带来的平台差异也给集中式模型带来诸多困难。因为每一种攻击行为在不同的操作环境中都表现出不同类型的模式特征，而已知的攻击方法数目非常多，因而在集中式模型的系统中，想要与攻击模式完全匹配就已经非常困难，何况还要应付不断出现的新型攻击手段。

面对诸多难题，很多新的思路已经出现，其中一种就是攻击策略分析(Attack Strategy Analysis)方法。它采用分布式智能代理的结构方式，由几个中央智能代理和大量分布的本地代理组成，其中本地代理负责处理本地事件，而中央代理负责整体的分析工作。与集中式模型不同的是，攻击策略分析强调的是通过全体智能代理协同工作来分析入侵者的攻击策略，中央代理扮演的是协调者和全局分析员的角色，但绝不是唯一的事件处理者，本地代理有较强的自主性，可以独立对本地攻击进行有效检测；同时也与中央智能代理和其他本地代理通信，接受中央智能代理的调度指挥，并与其他代理协同工作。这种方法有明显的优点，但同时又带来了其他的一些问题，如大量代理的组织和协作问题、相互之间的通信、处理能力和任务的分配等。

下面介绍一个典型的分布式入侵检测系统的解决方案。

图 7.5 所示的入侵检测系统是一种基于部件的分布式入侵检测系统。系统中的部件是具有特定功能的独立的应用程序，小型的系统或者仅仅是一个非独立的应用程序的功能模块。在部署时，这些部件可能在同一台计算机上，也可能各自分布在一个大型网络的不同部位，每个部件都能够完成某一特定的功能。各个部件之间通过统一的网络接口进行信息交换，这样既简化了数据交换的复杂性，使得多个部件能够很容易地分布在不同主机上，也给系统提供了一个扩展接口。



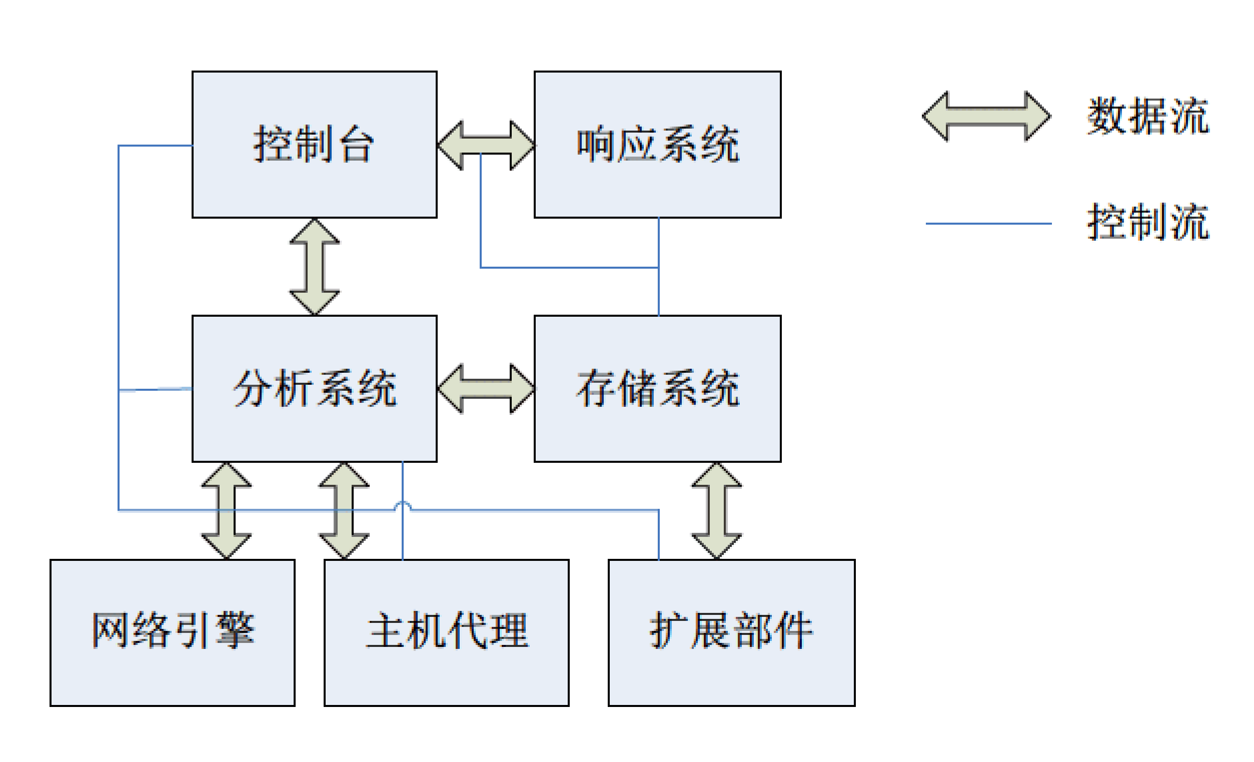


图 7.5　分布式入侵检测系统框图

系统主要部件有网络引擎(Network Engine)、主机代理(Host Agent)、存储系统(Storage System)、分析系统(Analyzer)、响应系统(Response System)和控制台(Manager Console)。

(1) 网络引擎和主机代理属于 CIDF 中的事件产生器(Event Generators)。网络引擎截获网络中的原始数据包，并从中寻找可能的入侵信息或其他敏感信息。主机代理从所在主机内收集信息，包括分析日志、监视用户行为、分析系统调用及分析该主机的网络通信等。网络引擎和主机代理也具有数据分析功能，对于已知的攻击，在这些部件中使用模式匹配的方法来检测，可以大大提高系统的处理速度，也可以减少分析部件的工作量及系统网络传输的影响。

(2) 存储系统用来存储事件产生器捕获的原始数据、并分析结果等，储存的原始数据用于对入侵者进行法律制裁时提供确凿的证据。存储系统也是不同部件之间数据处理的共享数据库，为系统不同部件提供各自感兴趣的数据。因此，存储系统应该提供灵活的数据维护、处理和查询服务，同时也必须是一个安全的日志系统。

(3) 分析系统能够对事件发生器捕获的原始信息，其他入侵检测系统提供的可疑信息进行统一分析和处理。分析系统采用高层次的分析方法，如基于统计的分析方法、基于神经网络的分析方法等，负责分布式攻击检测。

(4) 分析系统是整个入侵检测系统的大脑，分析方法则是该系统的思维能力。各种分析方法都有各自的优势和不足，因此，系统中分析方法应该是可以动态更换的，并且多种算法可以并存。

(5) 响应系统用于对确认的入侵行为采取相应措施。响应包括消极的措施，如给管理员发 E-mail、消息、传呼等；也可以采取保护性措施，如切断入侵者的 TCP 连接、修改路由器的访问控制策略等；还可以采取主动的反击策略，如对攻击者进行 DDoS 攻击等，但这种以毒攻毒的方法在法律上是不许可的。

(6) 控制台是整个入侵检测系统和用户交互的界面。用户可以提供控制台配置系统中的各个部件，也可以通过控制台了解各部件的运行情况。

7.5　入侵检测系统与协同

由入侵检测系统的基本构成可以看出，典型的入侵检测系统模型包括以下 3 个功能部件。

① 提供事件记录流的信息源。

② 发现入侵迹象的分析引擎。

③ 基于分析引擎的分析结果产生反应的响应部件 。

目前的入侵检测系统是网络安全整体解决方案的一个重要组成部分，需要与其他安全设备之间协同工作，共同解决网络安全问题，这就对引入协同提出了要求。

7.5.1　数据采集协同

入侵检测需要采集动态数据(网络数据包)和静态数据(日志文件等)。基于网络的入侵检测系统，仅在网络层通过原始的 IP 包进行监测，已不能满足日益增长的安全需求；基于主机的入侵检测系统，通过直接查看用户行为和操作系统日志数据来寻找入侵者，却很难发现来自底层的网络攻击。

目前的入侵检测系统将网络数据包的采集、日志文件的采集与信息分析割裂开来，即使是综合基于网络和基于主机的入侵检测系统也不例外，没有在这两类原始数据的相关性上加以考虑。此外，在采集网络数据包时，入侵检测系统一直是通过嗅探等被动方式来获取数据，一旦某个数据包丢失就无法挽回。而且，未来的网络是全交换的网络，网络速度越来越快，许多重要的网络还是加密的。在这种情况下，对动态网络数据包的采集就更加困难。因此，在数据采集上进行协同并充分利用各层次的数据，是提高入侵检测能力的首要条件。

数据采集协同包含以下几个方面的内容。

(1) 入侵检测系统与漏洞扫描系统的协同。漏洞扫描系统的特点是利用完整的漏洞库，对网络中的各个主机进行扫描，对主机所存在的网络、操作系统和运行等方面存在的漏洞给出综合报告，然后提出漏洞的修补办法和风险评估报告。

(2) 入侵检测系统与扫描系统的协同。一方面是可以利用扫描系统的扫描结果，对目前网络或系统所存在的漏洞做到心中有数，并对预警策略进行修改，从而尽可能地减少误报，并对隐含在正常行为中的攻击行为做出报警。另一方面，入侵检测系统能够对目前正在遭受攻击的漏洞进行及时防范。此外，漏洞扫描系统也可以利用入侵检测系统的报警信息，扫描主机的特定漏洞，查看正在受攻击的漏洞是否真实存在，如果真实存在，做出必须及时封堵的报告。

(3) 入侵检测系统与防病毒系统的协同。面对来自网络的病毒攻击，入侵检测系统可能根据某些特征做出警告，但由于入侵检测系统本身并不是防病毒系统，对网络中的主机是否真的正在遭受计算机病毒的袭击不能准确地预报，这时防病毒系统就有了用武之地，可以有针对性地对入侵检测系统的病毒报警信息进行验证，对遭受病毒攻击的主机系统进行适当的处理。

7.5.2　数据分析协同

入侵检测不仅需要利用模式匹配和异常监测技术来分析某个监测引擎所采集的数据，还要在此基础上利用数据挖掘技术，分析多个监测引擎提交的审计数据以发现更为复杂的入侵行为。



从理论上讲，任何网络入侵行为都能够被发现，因为网络流量和主机日志记录了入侵的活动。数据分析协同需要在两个层面上进行：一是对一个监测引擎采集的数据进行协同分析，综合使用监测技术，以发现较为常见的、典型的攻击行为； 二是对来自多个监测引擎的审计数据，利用数据挖掘技术进行分析，以发现较为复杂的攻击行为。考核入侵检测系统数据分析能力可以从准确性、效率和可用性 3 个方面进行。基于这一点，可以认为监测引擎是完成第一种数据分析协同的最佳地点，中心管理控制平台则是完成第二种数据分析协同的最佳地点。

当监测引擎面对并非单一的数据时，综合使用各种监测技术就显得十分重要。从攻击的特征来看，有的攻击方法使用异常监测来监测会很容易，而有的攻击方法使用模式匹配来监测则很简单。因此，对监测引擎的设计者来说，首先需要确定监测策略，明确哪些攻击行为属于异常监测的范畴，哪些攻击属于模式匹配的范畴。中心管理控制平台执行的是更为高级的、复杂的入侵检测，它面对的是来自多个监测引擎的审计数据，并可就各个区域内的网络活动情况进行“相关性”分析，其结果为下一时间段及监测引擎的监测活动提供支持。例如，黑客在正式攻击网络之前，往往利用各种探测器分析网络中最脆弱的主机及主机上最容易被攻击的漏洞，在正式攻击时，因为黑客的“攻击准备”活动早已被系统记录，所以入侵检测系统就能及时地对此攻击活动做出判断。

传统的数据挖掘技术的监测模型是离线产生的，这是因为传统数据挖掘技术的学习算法必须要处理大量的审计数据，十分耗时。但是，有效的入侵检测系统必须是实时的，而且基于数据挖掘的入侵检测系统仅仅在监测率方面高于传统方法的监测率是不够的，只有误报率也在一个可接受的范围内时才是可用的。

美国哥伦比亚大学提出了一种基于数据挖掘的实时入侵检测技术，证明了数据挖掘技术能够用于实时的入侵检测系统。基本框架是，首先从审计数据中提取特征，以帮助区分正常数据和攻击行为；然后将这些特征用于模式匹配或异常监测模型；接着描述一种人工异常产生方法，来降低异常监测算法的误报率；最后提供一种结合模式匹配和异常监测模型的方法。实验表明，上述方法能够提高系统的监测率，而不会降低任何一种监测模型的性能。在此技术基础上，实现数据挖掘的实时入侵检测系统是由引擎、监测器、数据仓库和自适应模型产生 4 部分构成，如图 7.6 所示。

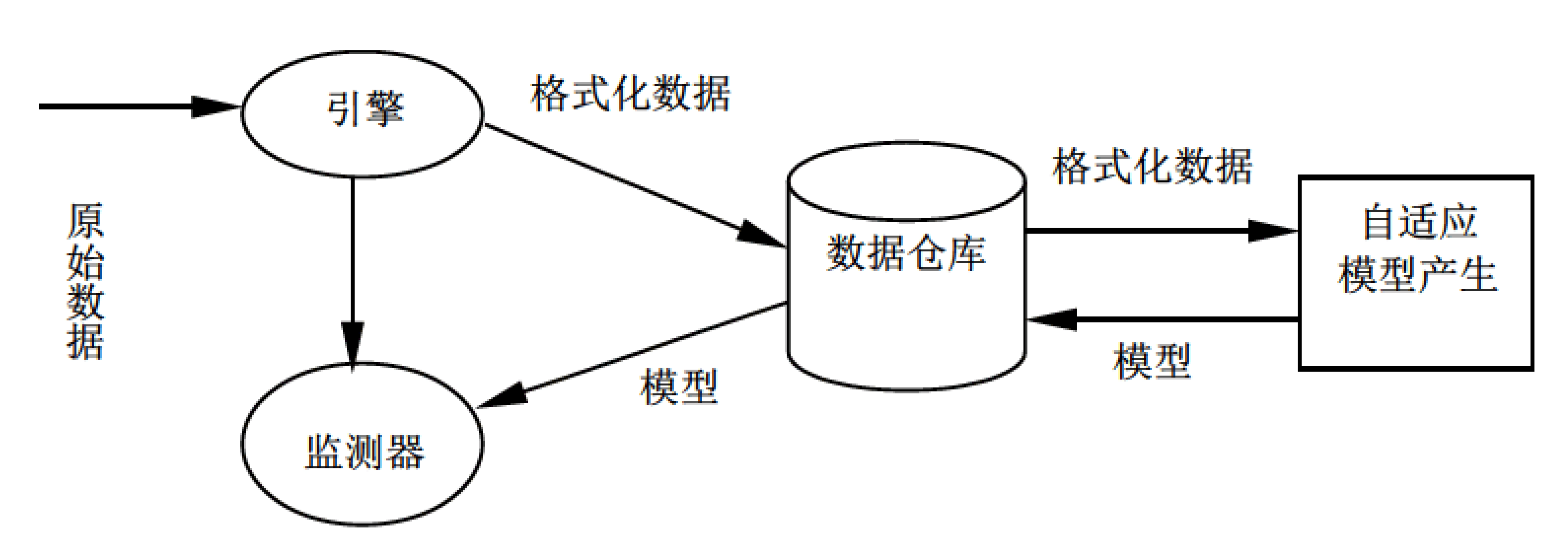


图 7.6　基于数据挖掘的入侵检测系统体系结构

在图 7.6 中，引擎观察原始数据并计算用于模型评估的特征；监测器获取引擎的数据并利用监测模型来评估其是否是一个攻击；数据仓库被用作数据和模型的中心存储地；自适应模型产生的主要目的是为了加快开发及分发新的入侵检测模型的速度。



7.5.3 响应协同

响应协同就是入侵检测系统与有充分响应能力的网络设备或网络安全设备集成在一起，构成响应和预警互补的综合安全系统。

响应协同主要包含以下几个方面。

1. 入侵检测系统与防火墙的协同

防火墙与入侵检测系统可以互补体现在静态和动态两个层面上。静态协同是指入侵检测系统可以通过了解防火墙的策略，对网络安全事件进行有效的分析，从而准确地报警，减少误报；动态协同是指当入侵检测系统发现攻击行为时，可以通知防火墙阻断已经建立的连接，同时通知防火墙修改策略，防止潜在的进一步攻击的可能性。

2. 入侵检测系统与路由器、交换机的协同

交换机和路由器一般串接在网络上，都有预定的策略，可以决定网络上的数据流，所以入侵检测系统与交换机、路由器的协同也有动态和静态两个方面，过程也大致相同，这里不再详述。

3. 入侵检测系统与防病毒系统的协同

对防病毒系统来讲，查毒和杀毒缺一不可，在查毒层面有数据采集协同，在杀毒层面有响应协同。入侵检测系统可以通过发送大量 RST 报文阻断已经建立的连接，但在防止计算机遭受病毒袭击的方面无能为力。目前由于网络病毒攻击所占比例不断增加，入侵检测系统与防病毒系统的协同也变得越来越重要。

4. 入侵检测系统与蜜罐和填充单元系统协同

蜜罐是试图将攻击者从关键系统引诱开的诱骗系统。这些系统充满了看起来很有用的信息，但是这些信息实际上是捏造的，合法用户是访问不到的。因此，当监测到对“蜜罐”的访问时，很可能就有攻击者闯入。“蜜罐”上的监控器和事件日志器监测这些未经授权的访问，并收集攻击者活动的相关信息。

利用“蜜罐”的这种能力，一方面可以为入侵检测系统提供附加数据；另一方面当入侵检测系统发现有攻击者时，可以把攻击者引入“蜜罐”，防止攻击者造成危害，并收集攻击者的信息。

“填充单元”采取另一种不同的方法。“填充单元”不是试图用引诱性的数据吸引攻击者，而是等待传统的入侵检测系统来监测攻击者，攻击者被传递到一个特定的填充单元主机，并处于一个模拟环境中，因此不会造成任何伤害。与“蜜罐”相似，这种模拟环境会充满使人感兴趣的数据，从而会使攻击者相信攻击正按计划进行。“填充单元”为监测攻击者的行为提供了独特的机会。

图 7.7 即为上述整个安全系统的示意图。

图 7.7 无法表示所有的数据流，只是形象地说明安全单元是一个网络安全整体。说明了入侵检测系统需要协同，同时其他所有的安全工具也需要协同，协同工作的目的是保障信息系统的安全。可以把所有这些协同工作的工具或者设备整体看作一个安全工具，它可



以保证信息有相对的安全性。

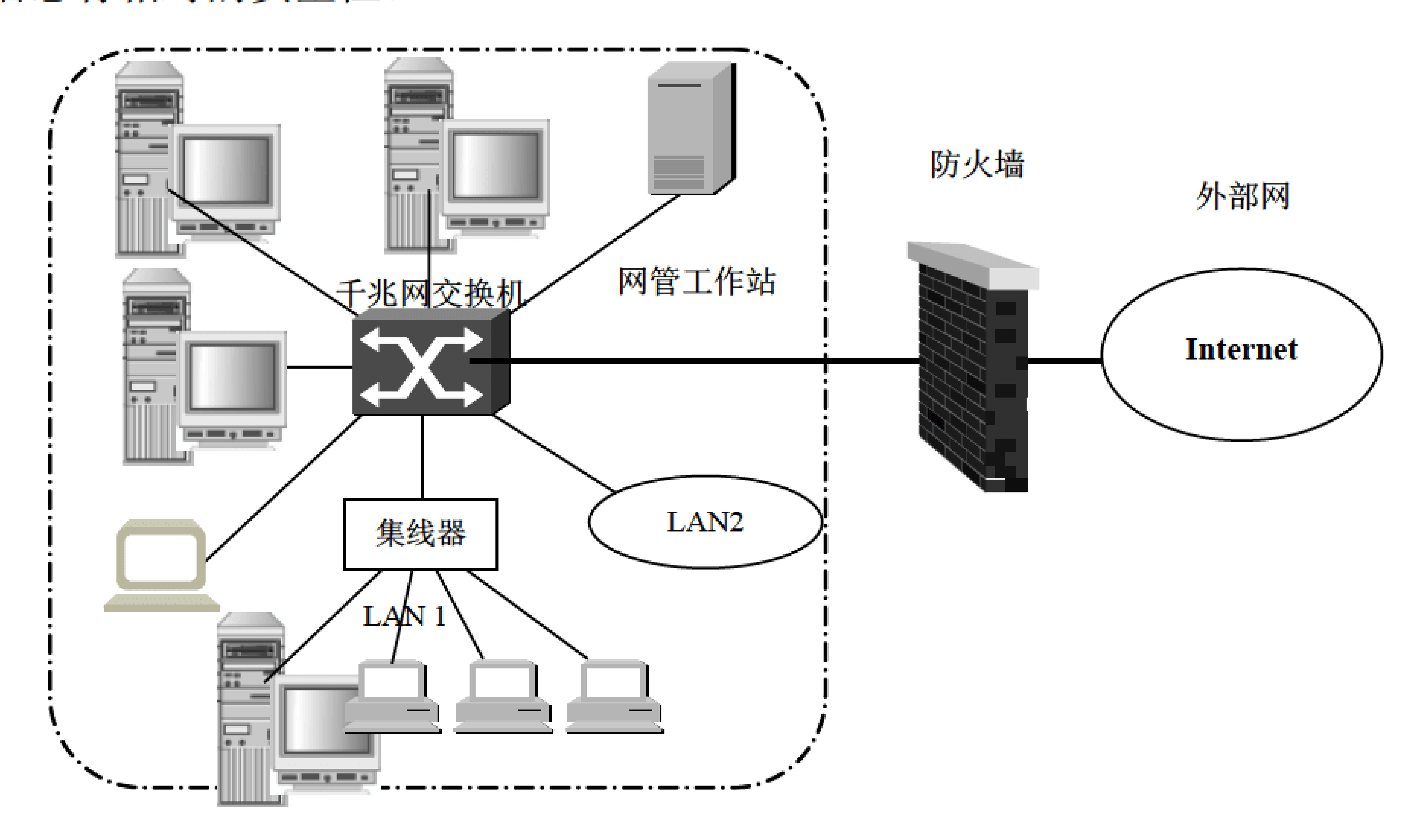


图 7.7　网络安全系统示意图

7.6　入侵检测分析

入侵检测技术是一种当今非常重要的动态安全技术，如果与传统的静态安全技术共同使用，可以大大提高系统的安全防护水平。

一个安全系统至少应该满足用户系统的保密性、完整性及可用性要求。但是，随着网络连接的迅速扩展，特别是互联网大范围的开放以及金融领域网络的接入，使越来越多的系统遭受到入侵攻击的威胁。这些威胁大多是通过挖掘操作系统和应用服务程序的弱点或者缺陷来实现的。

对付破坏系统企图的理想方法是建立一个完全安全的系统。这不仅要求所有的用户能识别和认证自己，而且还要求用户采用各种各样的加密技术和强制访问控制策略来保护数据。实际上这一点是很难做到的。

(1)　要将所有已安装的带安全缺陷的系统转换成安全系统是不现实的，即使真正付诸实践，也需要相当长的时间。

(2)　加密技术本身存在一定的问题。比如密钥的生成、传输、分配和保存以及加密算法的安全性。

(3)　访问控制和保护模型本身存在一定的问题。

(4)　静态的安全控制措施不足以保护安全对象属性。通常，安全访问控制等级和用户的使用效率成反比。在一个系统中，担保安全特性的静态方法可能会过于简单、不充分，或者是系统过度地限制用户。例如，静态安全措施未必能阻止违背安全策略造成的对数据文件的浏览；强制访问控制仅允许用户访问具有合适通道的数据，造成系统使用的不便。因此，动态的安全措施(如行为跟踪)对检测和尽可能地阻止入侵是必要的。

(5)　安全系统易受内部用户滥用特权的攻击。一些安全技术(如防火墙)能够防止一些外部攻击，但对来自内部的攻击就无能为力。

(6) 在实践中，建立完全安全的系统是不可能的。现今的操作系统和应用程序中不可能没有缺陷。在软件工程中存在着软件测试不充足、软件生命周期缩短等问题。

由于市场竞争激烈，软件生命周期正不断地被缩短，这样常常导致软件设计或测试不充分。并且有些软件的规模越来越大，复杂度越来越高，运行中用户的操作行为、软件安装平台、软件与软件之间交互的不可控性都可能带来问题。虽然，软件商经常会针对某些具体缺陷发布一些修补软件，但系统的安全状态只持续一段时间。此外，设计和实现一个整体安全系统也相当困难。

基于上述几类问题的解决难度，实用的方法是建立比较容易实现的安全系统，同时按照一定的安全策略建立相应的安全辅助系统。入侵检测系统就是这样一类系统。安全软件的开发方式基本上就是按照这个思路进行的。就目前系统安全状况而言，系统存在被攻击的可能性。如果系统遭到攻击，只要尽可能地检测到，甚至是实时地检测到，然后采取适当的处理措施，就可以避免造成更大的损失。

过去，防范网络攻击最常用的方法是使用防火墙。为了更好地说明入侵检测的必要性，下面对入侵检测与防火墙做一个比较。

“防火墙”是在被保护网络周边建立的、分隔被保护网络与外部网络的系统。防火墙技术是通过对网络作拓扑结构和服务类型上的隔离来加强网络安全的一种手段。他的保护对象是网络中有明确闭合边界的网块，防范对象则是来自被保护网块外部的对网络安全的威胁。防火墙通过在网络边界上建立相应的网络通信监控系统，拒绝非法的连接请求，从而达到保护网络安全的目的。

采用防火墙技术的前提条件如下。

(1) 被保护的网络具有明确定义的边界和服务。

(2) 网络安全的威胁仅来自外部网络。

通过监测、限制或更改穿过防火墙的数据流，尽可能地对外部网络屏蔽有关被保护网络的信息和结构，可实现对网络的安全保护，降低网络安全的风险。但仅仅使用防火墙保障网络安全是远远不够的。首先，防火墙本身会有各种漏洞和后门，有可能被外部黑客攻破；其次，防火墙不能阻止内部攻击，对内部入侵者来说防火墙毫无作用；另外，有些外部访问可以绕开防火墙，如内部用户通过调制解调器拨号接入 Internet，从而开辟了一个不安全的通路，而这一连接并没有通过防火墙，防火墙对此没有任何监控能力。

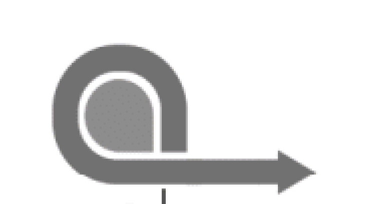
因此，仅仅依赖防火墙系统并不能保证足够的安全。入侵检测是防火墙的合理补充，为网络安全提供实时的入侵检测并采取相应的防护手段，如记录证据用于跟踪入侵者和灾难恢复、发出警报甚至终止进程、断开网络连接等。它从计算机网络系统中的若干关键点收集信息，并分析这些信息，检查网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下，能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。

入侵检测系统一般不是采取预防的措施以防止入侵事件的发生，入侵检测作为安全技术其主要目的如下。

(1) 识别入侵者。

(2) 识别入侵行为。

(3) 检测和监视已成功的安全突破。



(4) 为对抗入侵，及时提供重要信息，阻止事件的发生和事态的扩大。

可见，入侵检测对于建立一个安全系统来说是非常必要的，它可弥补传统安全保护措施的不足。

作为一类目前备受关注的网络安全技术，入侵检测技术也有很多不足。

(1) 入侵检测系统本身还在迅速发展和变化，尚未成熟。目前，绝大多数的商业入侵检测系统的工作原理和病毒检测相似，其自身带有一定规模和数量的入侵特征模式库，可以定期更新。这种方式有很多弱点：不灵活，仅对已知的攻击手段有效；特征模式库的提取和更新依赖于手工方式，维护不易；具有自适应能力、能自我学习的入侵检测系统还尚未成熟，检测技术在理论上还有待突破。所以入侵检测系统领域当前正处于不断发展成长时期。

(2) 现有的入侵检测系统错报率(或称为虚警率)偏高，严重干扰了检测结果。如果入侵检测系统对原本不是攻击的事件产生了错误的警报，则假的警报一般称为虚警(False Positive)。通常这些错报会干扰管理员的注意力，产生两种后果：

① 忽略警报，但这样做的结果和安装入侵检测系统的初衷相背；

② 重新调整临界阈值，使系统对虚报的事件不再敏感，但这样做之后，一旦有真的相关攻击事件发生，入侵检测系统将不再报警，这同样损失了入侵检测系统的功效。

(3) 事件响应与恢复机制不完善。这一部分对入侵检测系统非常重要，但目前几乎都被忽略并且没有一个完善的响应恢复体系，远不能满足人们的期望和要求。

(4) 入侵检测系统与其他安全技术的协作性不够。如今，网络系统中往往采用很多其他的安全技术，如防火墙、身份认证系统、网络管理系统等。如果它们之间能够相互沟通、相互配合，对入侵检测系统进一步增强自身的检测和适应能力是有帮助的。

(5) 入侵检测系统缺少对检测结果做进一步说明和分析的辅助工具，这妨碍了用户进一步理解看到的数据或图表。

(6) 入侵检测系统缺乏国际统一的标准。

① 没有关于描述入侵过程和提取攻击模式的统一规范。

② 没有关于检测和响应模型的统一描述语言。

③ 检测引擎的定制处理没有标准化。

7.7 入侵检测的发展

7.7.1 入侵检测标准

入侵检测技术的标准化是提高入侵检测产品功能和加强技术合作的重要手段，到目前为止，还没有一个被广泛接受的入侵检测相关国际标准。美国国防部高级研究计划署(DARPA)和互联网工程任务组(IETF)的入侵检测工作组(IDWG)在这方面做了很多工作，我国的有关网络安全产品检测部门也做了很多卓有成效的工作，给出了主机入侵检测产品和网络入侵检测产品的规范。

IDWG 提出的建议草案包括 3 部分内容，即入侵检测消息交换格式(IDMEF)、入侵检测交换协议(IDXP)和隧道轮廓(Tunnel Profile)。

(1) IDMEF 描述了入侵检测系统输出信息的数据模型，并解释了使用此模型的基本原理。该数据模型用 XML 实现，并设计了一个 XML 文档类型定义。自动入侵检测系统可以使用 IDMEF 提供的标准数据格式对可疑事件发出警报，提高商业、开放资源和研究系统之间的互操作性。IDMEF 最适用于入侵检测分析器(或称为"探测器")和接收警报的管理器(或称为"控制台")之间的数据信道。

(2) IDXP 是一个用于入侵检测实体之间交换数据的应用层协议，能够实现 IDMEF 消息、非结构文本和二进制数据之间的交换，并提供面向连接协议之上的双方认证、完整性和保密性等安全特征。IDXP 是 BEEP 的一部分，后者是一个用于面向连接的异步交互通用应用协议，IDXP 的许多特色功能(如认证、保密性等)都是由 BEEP 框架提供的。

7.7.2　入侵检测评测

以下从对入侵检测评估的作用、测试评估入侵检测系统的标准和测试评估现状等几个方面对入侵检测评估进行介绍。

1. 对入侵检测系统进行测试和评估的作用

(1) 有助于更好地描述入侵检测系统的特征。通过测试评估，可以更好地认识、理解入侵检测系统的处理方法、所需资源及环境，建立比较入侵检测系统的基准，领会各检测方法之间的关系。

(2) 对入侵检测系统的各项性能进行评估，确定入侵检测系统的性能级别及其对运行环境的影响。

(3) 利用测试和评估结果，可作出一些预测，推断入侵检测系统发展的趋势，评估风险，制定可实现的入侵检测系统质量目标(如可靠性、可用性、速度、精确度等)、花费及开发进度。

(4) 根据测试和评估的结果，对入侵检测系统进行改善，即发现系统中存在的问题并进行改进，从而提高系统的各项性能指标。

2. 测试评估入侵检测系统性能的标准

(1) 准确性。准确性(Accuracy)指入侵检测系统从各种行为中正确地识别入侵的能力，当一个入侵检测系统的检测不准确时，就有可能把系统中的合法活动当作入侵行为，并标识为异常(虚警现象)。

(2) 处理性能。处理性能(Performance)指一个入侵检测系统处理源数据的速度。当入侵检测系统的处理性能较差时，就不可能实现实时的入侵检测系统，反而可能成为整个系统的瓶颈，进而严重影响整个系统的性能。

(3) 完备性。完备性(Completeness)指入侵检测系统能够检测出所有攻击行为的能力。如果有一个攻击行为，无法被入侵检测系统检测出来，那么该入侵检测系统就不具有检测完备性，也就是说，它把对系统的入侵活动当作正常行为(漏报现象)。由于攻击类型、攻击手段变化很快，很难得到关于攻击行为的所有知识，所以关于入侵检测系统的检测完备性的评估相对比较困难。

(4) 容错性。由于入侵检测系统是检测入侵的重要手段，所以它成为很多入侵者攻击



的首选目标。入侵检测系统自身必须能够抵御对他自身的攻击，特别是拒绝服务(Denial-of-Service)攻击。由于大多数的入侵检测系统是运行在极易遭受攻击的操作系统和硬件平台上，这就使得系统的容错性(Fault Tolerance)变得特别重要，在测试评估入侵检测系统时必须考虑到这一点。

(5) 及时性。及时性(Timeliness)要求入侵检测系统必须尽快地分析数据，并把分析结果传播出去，以使系统安全管理者能够在入侵攻击尚未造成更大危害以前做出反应，阻止入侵者进一步的破坏活动。与处理性能因素相比，及时性的要求更高，它不仅要求入侵检测系统的处理速度要尽可能快，而且要求传播、反映检测结果信息的时间尽可能短。

美国加州大学的 Nicholas J.Puketza 等人把测试分为 3 类，分别与前面的性能指标相对应，即入侵识别测试(入侵检测系统有效性测试)、资源消耗测试(Resource Usage Tests)及强度测试。入侵识别测试测量入侵检测系统区分正常行为和入侵行为的能力，主要指标是检测率和虚警率；资源消耗测试测量入侵检测系统占用系统资源的状况，考虑的主要因素是硬盘占用空间、内存消耗等；强度测试主要检测入侵检测系统在强负荷运行状况下检测效果是否受到影响，主要包括大负载、高密度数据流量情况下对检测效果的检测。

3. 入侵检测系统测试评估现状及存在的问题

虽然入侵检测系统及其相关技术已获得了很大的进展，但关于入侵检测系统的性能检测及其相关评测工具、标准以及测试环境等方面的研究工作还很缺乏。

在测试评估过程中，采用模拟的方法来生成测试数据，而模拟入侵者实施攻击面临的困难是只能掌握已公布的攻击，而对于新的攻击方法就无法得知。这样的后果是，即使测试没有发现入侵检测系统的潜在弱点，也不能说明入侵检测系统是一个完备的系统。不过，可以通过分类选取测试例子，使之尽量覆盖各种不同种类的攻击，同时不断更新入侵知识库，以适应新的情况。

此外，由于测试评估入侵检测系统的数据都是公开的，如果针对测试数据设计待测试的入侵检测系统，则该入侵检测系统的测试结果肯定比较好，但这并不能说明它实际运行的状况就好。

入侵检测作为一门正在蓬勃发展的新兴技术，出现的时间并不是很长。相应地，对入侵检测技术进行评测出现得更晚，它肯定有很多不完善和有待改进的地方。几个比较关键的问题是网络流量仿真、用户行为仿真、攻击特征库的构建、评估环境的构建以及评测结果的分析等。

7.7.3　入侵检测发展

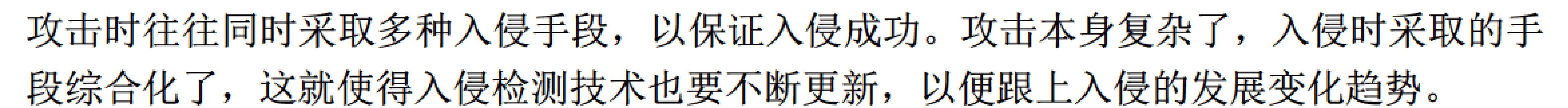
1. 入侵技术的发展

近年来，系统和网络的漏洞被不断发现，入侵技术无论是从规模上还是方法上都发生了变化，入侵的手段与技术也有了“进步与发展”，这种“进步与发展”直接加速了人们对入侵检测系统的研究和推广工作。

从最近几年的发展趋势看，入侵技术的发展与演化主要反映在以下几个方面。

1) 入侵和攻击的复杂化与综合化

由于网络防范技术的进步和多元化，使得攻击的难度增加，因此入侵者在实施入侵或



攻击时往往同时采取多种入侵手段，以保证入侵成功。攻击本身复杂了，入侵时采取的手段综合化了，这就使得入侵检测技术也要不断更新，以便跟上入侵的发展变化趋势。

2) 入侵主体的间接化

入侵主体的间接化，即实施入侵和攻击的主体的隐蔽化，通过一定的技术，可掩盖攻击主体的源地址及主机位置。使用隐蔽技术后，对于被攻击对象来说，攻击的主体是无法直接确定的。现在有不少攻击都是借助其他脆弱主机或网络来攻击目标主机，而他们自己却隐藏在背后，因此不容易被发现和查出，即使能够发现攻击，也不一定能够有效地追踪到攻击者。一般的攻击者在攻击别人时，肯定不希望自己的攻击被发现，至少是自己的真实 IP 地址不被追踪到，因此，他们会想方设法地掩盖自己的行踪。

3) 入侵和攻击的规模扩大

在初期，入侵和攻击往往是针对某一个公司或网站，其攻击的目的常常是某些网络技术爱好者的猎奇行为，当然也不排除商业的盗窃与破坏行为。现在的攻击主要是针对网络的，也就是说，他们的目的就是要使目标网络崩溃或瘫痪，这样造成的危害更严重、波及面更广。此外，由于战争对电子技术与网络技术的依赖性越来越大，未来战争中的电子战与信息战将不可避免。对于信息战，无论其规模与技术都与一般意义上的计算机网络的入侵与攻击不可相提并论。信息战的成败、国家主干通信网络的安全就像国家的领土安全一样不容忽视。

4) 入侵和攻击技术的分布化

以前常用的入侵与攻击行为往往由单机执行，由于防范技术的发展使得此类行为不能奏效。因此，攻击者现在多采取使用主机同时攻击一台机器的办法，这就是分布式拒绝服务攻击(DDoS)，它能够在很短的时间内造成被攻击主机瘫痪。DDoS 攻击通过控制数台脆弱主机，将其武装成为一台极具攻击力的攻击者，然后同时对目标主机发起攻击。由于此类分布式攻击的单机信息模式与正常通信没有差异，使用通常的入侵检测方法无法及时检测出攻击，所以往往在攻击发动的初期不能被发现。

5) 攻击对象的转移

入侵与攻击常以网络为侵犯的主体，但近期攻击行为却发生了策略性的改变，由攻击网络改为攻击网络的防护系统，且愈演愈烈。攻击者详细地分析了入侵检测系统的审计方式、特征描述、通信模式，从中找出入侵检测系统的弱点，然后加以攻击。入侵者一旦攻破入侵检测系统等安全部件，能够长驱直入，肆无忌惮地攻击目标主机，其攻击行为无法得到记录，很难取证，因此也就很难得到应有的惩罚。

2. 入侵检测技术的发展

以下是入侵检测技术发展的几个重要方向。

1) 功能与性能提高

为提高检测准确率，其他领域的一些概念和方法被引入到入侵检测系统中，如神经网络、模糊理论、免疫系统、数据挖掘等。这些方法主要是为了增强入侵检测系统的学习能力，使得入侵检测系统可以比较智能地检测出未知攻击。但这些方法基本上还都处于研究阶段，入侵检测系统产品还没有很好地实现这些方法。

此外，网络速度也构成了对检测准确率的挑战之一。现在网络的规模越来越大，入侵



检测系统应用的场合也越来越广，网络的速度在不断提高，因此，入侵检测系统产品必须能够适应高速网络发展的要求，否则就会出现大量的漏报现象。为了能够适应高速网络的要求，入侵检测系统中现有的一些技术将不得不进行改进，有的将被弃用。

因此，改进现有的入侵检测方法，提出新的、可以应用于大规模高速网络的入侵检测方法，对于适应新的应用需要，提高入侵检测系统的准确率非常必要。

2) 检测和防范分布式攻击和拒绝服务攻击

由于分布式攻击隐蔽性强、攻击力大，因此现在使用分布式攻击进行入侵的情况越来越多，而现在的入侵检测系统产品对于分布式攻击的防范能力普遍较弱。如何准确地描述分布式攻击，检测到可疑攻击后，又如何将分开的攻击特征合并，从中确定分布式攻击，都是值得认真研究的课题。

3) 实现入侵检测系统与其他安全部件的协同

实现网络与信息的安全是一项系统工程，不是某一种单独的安全部件就可以完成的。只有在不同的安全部件之间实现协同工作，才能更好地发挥他们各自的作用，才能进一步保证网络与信息的安全。

4) 入侵检测系统的标准化工作

尽管入侵检测系统经历了 20 多年的发展，近几年又成为网络与信息安全领域的一个研究热点，但到目前为止，尚没有一个相关的国际标准出现，国内也没有入侵检测系统方面的标准。入侵检测系统的标准化工作必将成为业界关注的热点。

5) 入侵检测系统的测试和评估

对于入侵检测系统的测试和评估，虽然不是入侵检测系统本身的技术，但对于促进入侵检测系统的发展和入侵检测系统产品的推广非常重要。

以上从 5 个方面介绍了入侵检测系统研究中尚待解决的技术问题，这些问题的解决将会大大促进入侵检测系统的发展。

复习思考题七

一、选择题

入侵防护系统的缩写是<u> ① </u>，<u> ② </u>是指计算机紧急响应小组，<u> ③ </u>是认证中心，而<u> ④ </u>是入侵检测系统的缩写。

(　　) ① A. IDS　B. IPS　C. CERT　D. CA

(　　) ② A. IDS　B. IPS　C. CERT　D. CA

(　　) ③ A. IDS　B. IPS　C. CERT　D. CA

(　　) ④ A. IDS　B. IPS　C. CERT　D. CA

二、问答题

1. 什么是入侵检测系统？它由哪些基本组件构成？
2. 简述入侵检测的功能和分类。
3. 简述常用的误用检测技术和异常检测技术的原理。
4. 比较异常检测和误用检测技术的优缺点。

5. 简述蜜罐和蜜网之间的关系。

6. 简述入侵响应技术的基本手段。

7. 比较基于网络和基于主机的入侵检测系统的优缺点。

8. 入侵检测系统与协同的含义是什么？主要协同类型有哪些？

9. 结合实际谈一谈当前入侵检测的现状与不足，以及下一代入侵检测应具有的良好特性。

10. 为什么说入侵检测是防火墙的合理补充?

第 8 章　VPN 与 NAT 技术及安全协议

学习目标

虚拟专用网络(VPN)指的是在公用网络上建立专用网络的技术。网络地址转换(NAT)属于接入广域网(WAN)技术，是一种将私有(保留)地址转化为合法 IP 地址的转换技术，它被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。通过本章的学习，应该达到以下学习目标:

- 熟练掌握 VPN 的概念及其采用的主要技术。
- 熟练掌握 NAT。

8.1　虚拟专用网 VPN

8.1.1　VPN 概述

虚拟专用网络(Virtual Private Network，VPN)指的是在公用网络上建立专用网络的技术。其之所以称为虚拟网，主要是因为整个 VPN 网络的任意两个节点之间的连接并没有传统专用网所需的端到端的物理链路，而是架构在公用网络服务商所提供的网络平台，如 Internet、ATM(异步传输模式)、Frame Relay (帧中继)等之上的逻辑网络，用户数据在逻辑链路中传输。它涵盖了跨共享网络或公共网络的封装、加密和身份验证链接的专用网络的扩展。VPN 主要采用了隧道技术、加/解密技术、密钥管理技术和使用者与设备身份认证技术。

VPN 是依靠 ISP(Internet 服务提供者)和其他 NSP(网络服务提供者)在公用网络中建立专用的数据通信网络的技术。它有两层含义：一是它是虚拟的网，即任意两个节点之间的连接并没有传统专用网所需要的端到端的物理链路，而是通过一个共享网络环境实现的，网路只有在用户需要时才建立；二是它利用公网的设施构成的专用网。这样一个网兼顾了公网和专网的许多优点，将公网的可靠、功能丰富与专网的灵活、高效结合在一起，是介于公网与专用网之间的一种网。

VPN 系统使分布在不同地方的专用网络在不可信任的公共网络(如因特网)上安全地通信。它采用复杂的算法来加密传输的信息，使得需要受保护的数据不会被窃取。一般来说，其工作流程大致如下：要保护的主机发送不加密信息到连接公共网络的 VPN 设备；后者根据网络管理员设置的规则，确认是否需要对数据进行加密或让数据直接通过；对需要加密的数据，VPN 设备对整个数据包(包括要传送的数据、发送端和接收端的 IP 地址)进行加密和附上数字签名；VPN 设备加上新的数据包头，其中包括目的地 VPN 设备需要的安全信息和一些初始化参数；VPN 设备对加密后数据、鉴别包以及源 IP 地址、目标 VPN 设备 IP 地址进行重新封装，重新封装后数据包通过虚拟通道在公网上传输；当数据包到达目标 VPN 设备时，数字签名被核对无误后数据包被解密。

典型的 VPN 结构是：若干个内部网络通过公网连接起来，各个内部网络位于 VPN 设

备的后面，同时通过路由器连接到公网。在这种 VPN 结构中，数据按照严密的算法在公网中通过多层的虚拟通道(也称“隧道”)，从一端 VPN 设备到达另一端。隧道从一个 VPN 设备开始，通过路由器横跨整个公网到达其他 VPN 设备。隧道的第二层要对数据进行加密封装，到达目标 VPN 设备后接收方得到的是重新封装后的数据。隧道的第三层主要任务是进行身份验证，采用不同的算法来验证信息来源的真实性。

下面来看一下 VPN 的优越性。

1)　建设成本低

VPN 的显著特点是用户能够用公共网络结构提供专用网络业务传输和服务，而一般不需要大量的投资，比建立真正的专用网的成本要低得多，投资风险也小。用户可以凭借公用网的环境，把属于自己的网络用户终端、有关的接入线路、模块及端口模拟成自己的专用网，并通过自己的网络管理设施对 VPN 进行管理，就像真正的专用网那样。

远程专用网络(Remote Private Network，RPN)的建造和维护非常昂贵，一般只有银行、跨国公司才有可能拥有。而 Internet 遍布世界各个角落，利用 Internet 可以节省网络建设的大部分开销，且只需付市话费用就可达到长途通信的效果。调查表明，利用 Internet 传输数据，公司可节省 50%的传统租用网络运行费用。

2)　容易扩展

企业只需依靠提供 VPN 服务的 ISP 就可以随时扩大 VPN 的容量和覆盖范围，自己需要做的事很少。

3)　使用方便

过去与合作伙伴联网，必须事先协商如何在双方之间建立租用线路或帧中继线路，VPN 出现之后，这种协商已毫无必要，真正达到了随意连接和断开。

4)　易于管理

VPN 使企业可以利用 ISP 的设施和服务，同时又完全自己掌握网络的控制权。例如，企业可以委托 ISP 提供拨号访问，由自己负责用户的查验、访问权、网络地址、安全性和网络变化管理等重要工作。

采用 VPN 还可将用户原有的专用网与之无缝地综合在一起，使用户可以实施混合的 VPN 方案；VPN 还具有灵活的计费方式，可以有各种方式接入，能满足不同的需要，具有统一的网络功能。

8.1.2　VPN 的分类

VPN 的分类有多种。按 VPN 的应用平台可分为软件平台 VPN、专用硬件平台 VPN 和辅助硬件平台 VPN；按构建 VPN 的隧道协议(第二层隧道协议、第三层隧道协议)又可分为 L2TP VPN、IPSec VPN 等；按 VPN 的部署模式又可分为端到端模式、供应商－企业模式和内部供应商模式等。通常根据业务类型，把 VPN 业务大致分为两类。

1. 拨号 VPN(VPDN)

拨号 VPN 是指企业员工或企业的小分支机构通过公网远程拨号的方式构筑的虚拟网。根据隧道发起方式它又分为由用户发起、由 ISP 拨号服务器发起及由企业网远程路由器发起三种。该 VPN 的核心是通过 L2TP 协议，来实现第二层的隧道封装。这样一来，企业员



工到 ISP 的各节点出差或办公时，可通过当地的市话直接拨号上网，并访问企业网。这一方式使得企业网可以真正管理自己的用户。企业员工不必在 ISP 上拥有自己的账号，也可以使用自己在企业网中的账号和口令拨号上网。从目前的情况看，运营商在实现 VPN 业务时，急需解决不同厂商设备的互操作性的问题以及认证、计费等问题。

2. 专线 VPN

专线 VPN 为用户提供的应是安全、可靠并具有 QoS 的 VPN。

专线 VPN 通常是由 IPSec 协议来实现的。IPSec 是一套完整的协议，它定义了在公网上安全传输数据的方式。IPSec 要防止网络上的窃听者对数据的篡改，并确保数据通信双方的身份，对数据进行安全加密。其中，通信双方加密密钥的交换、安全信任关系的确立是 IPSec 实现的关键。专线 VPN 另一个重要功能就是为用户提供 QoS 保障。

专线 VPN 又分内部网 VPN(Intranet VPN)和外联网 VPN(Extranet VPN)。内部网 VPN 是企业的总部与分支机构间通过公网构筑的虚拟网。外联网 VPN 是指多个具有合作伙伴关系的企业，通过公网来构筑的虚拟网。

VPN 使企业可以利用 ISP 的设施和服务，同时又完全自己掌握网络的控制权。例如，企业可以委托 ISP 提供拨号访问，由自己负责用户的查验、访问权、网络地址、安全性和网络变化管理等重要工作。

8.1.3 VPN 的 4 项技术

目前 VPN 主要采用 4 项技术，即隧道技术(Tunneling)、加/解密技术(Encryption & Decryption)、密钥管理技术(Key Management)、使用者与设备身份认证技术(Authentication)。

隧道技术是 VPN 的基本技术，类似于点对点连接技术，它在公用网建立一条数据通道(隧道)，让数据包通过这条隧道传输。隧道是由隧道协议形成的，分为第二层、第三层隧道协议。第二层隧道协议是先把各种网络协议封装到 PPP 中，再把整个数据包装入隧道协议中。这种双层封装方法形成的数据包靠第二层协议进行传输。第二层隧道协议有 L2F、PPTP、L2TP 等。L2TP 协议是目前 IETF 的标准，由 IETF 融合 PPTP 与 L2F 而形成。

第三层隧道协议是把各种网络协议直接装入隧道协议中，形成的数据包依靠第三层协议进行传输。第三层隧道协议有 VTP、IPSec 等。IPSec(IP Security)是由一组 RFC 文档组成，定义了一个系统来提供安全协议选择、安全算法，确定服务所使用密钥等服务，从而在 IP 层提供安全保障。

加/解密技术是数据通信中一项较为成熟的技术，VPN 可直接利用现有技术。

密钥管理技术的主要任务是如何在公用数据网上安全地传递密钥而不被窃取。现行密钥管理技术又分为 SKIP 与 ISAKMP/OAKLEY 两种。SKIP 主要是利用 Diffie-Hellman 的演算法则，在网络上传输密钥；在 ISAKMP 中，双方都有两把密钥，分别用于公用、私用。

身份认证技术最常用的是使用者名称与密码或卡片式认证等方式。

VPN 的连接过程首先由客户机向 VPN 服务器发出请求，VPN 服务器响应请求并向客户机发出身份质询，客户机将加密的响应信息发送到 VPN 服务器，VPN 服务器根据用户数据库检查该响应，如果账户有效，VPN 服务器将检查该用户是否具有远程访问权限，如果该用户拥有远程访问权限，VPN 服务器接受此连接。在身份验证过程中产生的客户机和

服务器公有密钥将用来对数据进行加密。VPN 连接的示意图如图 8.1 所示。

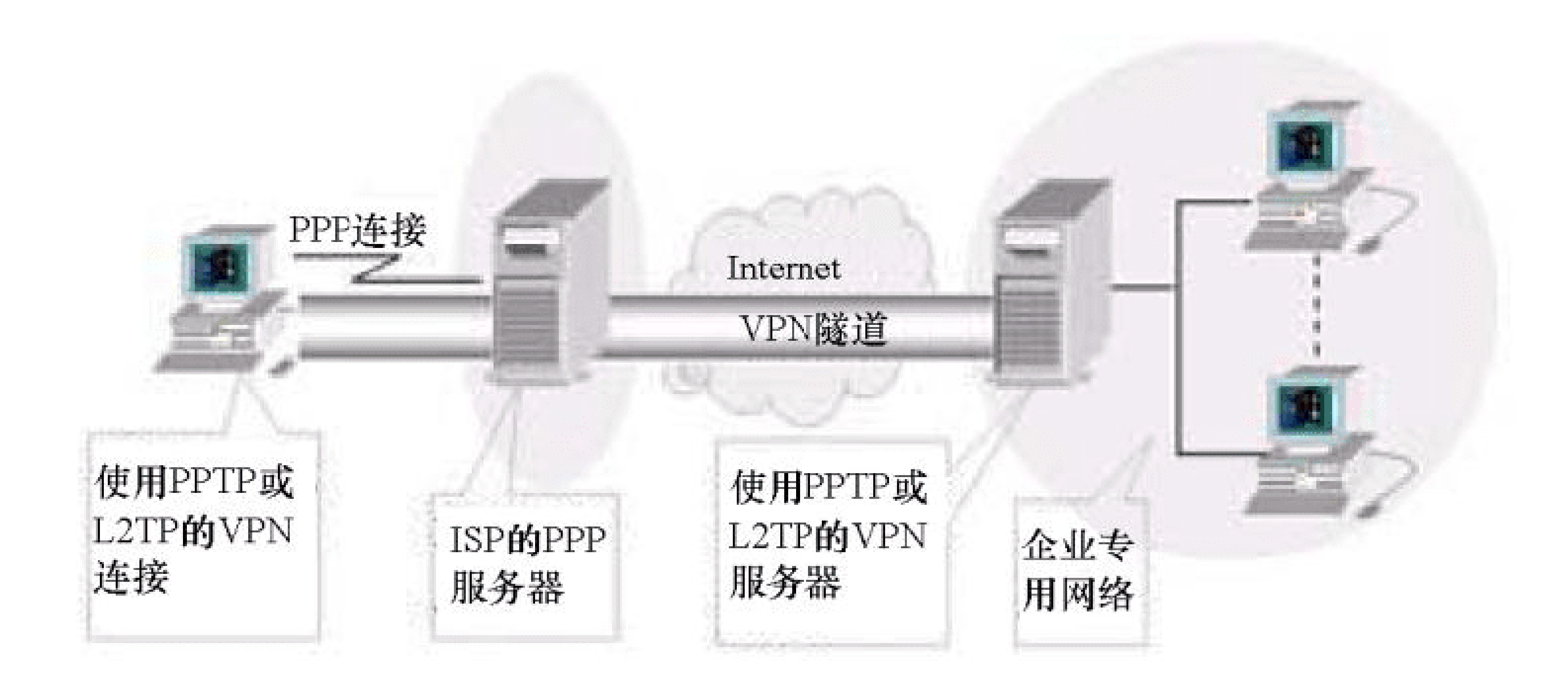


图 8.1　VPN 的连接示意图

8.1.4　VPN 的寻址和路由

要理解 VPN 的工作原理，则必须对 VPN 的寻址及路由有个基本认识。VPN 连接在建立的同时创建一个虚拟接口，该虚拟接口必须被分配适当的 IP 地址，同时需要对路由做修改或添加，以确保数据流是在安全的 VPN 连接上而不是在公共网络上传输。下面分别就远程访问 VPN 和路由器-路由器 VPN 这两种不同的连接方式介绍 VPN 的寻址和路由。

1. 远程访问 VPN 连接

在远程访问 VPN 连接建立过程中，VPN 服务器为远程访问 VPN 客户机分配一个 IP 地址并修改远程客户机上的默认路由，从而使得在默认情况下数据流可以经由虚拟接口发送。

1)　IP 地址和拨号 VPN 客户机

对于在创建 VPN 连接之前，需要以拨号方式上网的 VPN 客户机，有两个 IP 地址必须被分配。

(1)　创建 PPP 连接时，IPCP 与 ISP NAS 协商，分配一个公共 IP 地址。

(2)　创建 VPN 连接时，IPCP 与 VPN 服务器协商，分配一个 Intranet IP 地址。这个由 VPN 服务器分配的 IP 地址可以是一个公共 IP 地址，也可以是一个专用 IP 地址，具体情况依据不同的企业在其 Intranet 上所实现的是公共地址分配还是专用地址分配而定。

分配给 VPN 客户机的两个 IP 地址都必须是可以被 Intranet 中的主机找得到的；反之亦然。为了实现这一点，在 VPN 服务器的路由表中必须包含能找到 Intranet 中每一台主机的路由表条目，而在 Intranet 的路由器的路由表中也必须包含能找到所有 VPN 客户机的路由表条目。

如上所述，VPN 隧道数据将产生两个 IP 报头，其内部 IP 报头的源端和目的端地址分别是由 VPN 服务器分配的 VPN 客户机 IP 地址和 Intranet 地址；其外部 IP 报头中源端和目的端地址分别是由 ISP 分配的 VPN 客户机 IP 地址和 VPN 服务器的公共地址。由于 Internet 上的路由器仅处理外部 IP 报头，因此在 IP 网络上传输时，Internet 路由器将数据转发到 VPN 服务器的公共 IP 地址上。

图 8.2 给出了拨号客户机寻址示意图，其中，企业 Intranet 采用专用 IP 地址分配，传



输数据为 IP 数据报。

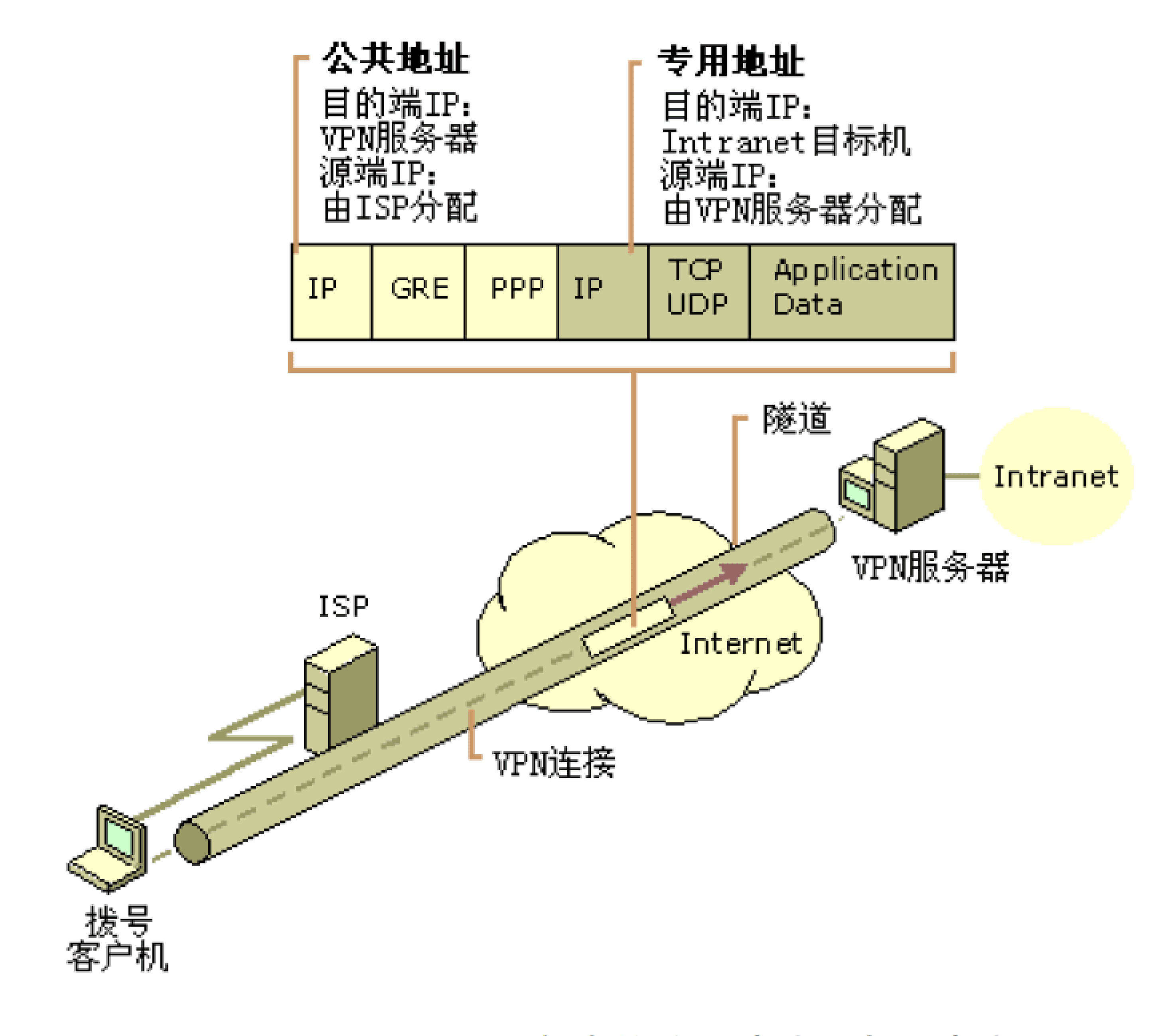


图 8.2　PPTP 数据包中的公共地址和专用地址

2)　默认路由和基于 Internet 的 VPN

如图 8.3 所示，拨号客户机拨打 ISP 时，利用至 ISP 的连接，客户机即添加了一条默认路由。这样，经由 ISP NAS 的路由器，客户机可以到达 Internet 上任意目标地址。

从图 8.3 中我们已经看到，客户机拨打 ISP 时会产生一条默认路由，而随后当 VPN 客户机创建 VPN 连接时，又将添加另一条直接至隧道服务器地址的默认路由和宿主机路由，如图 8.4 所示。前一条默认路由将被保存，但新的默认路由长度更长。添加新的默认路由意味着在一条 VPN 连接的有效连接期内，发自客户机的数据包只能到达隧道服务器的 IP 地址，而无法达到其他任何 Internet 目的地址。

生成两条默认路由的意义在于：

(1)　当 VPN 连接处于非活动状态时，发自客户机的数据包可到达任意 Internet 目的地址，但不能抵达 Intranet 目的地址。

(2)　当 VPN 连接处于活动状态时，发自客户机的数据包可到达 Intranet 目的地址，但不能抵达任何 Internet 目的地址。

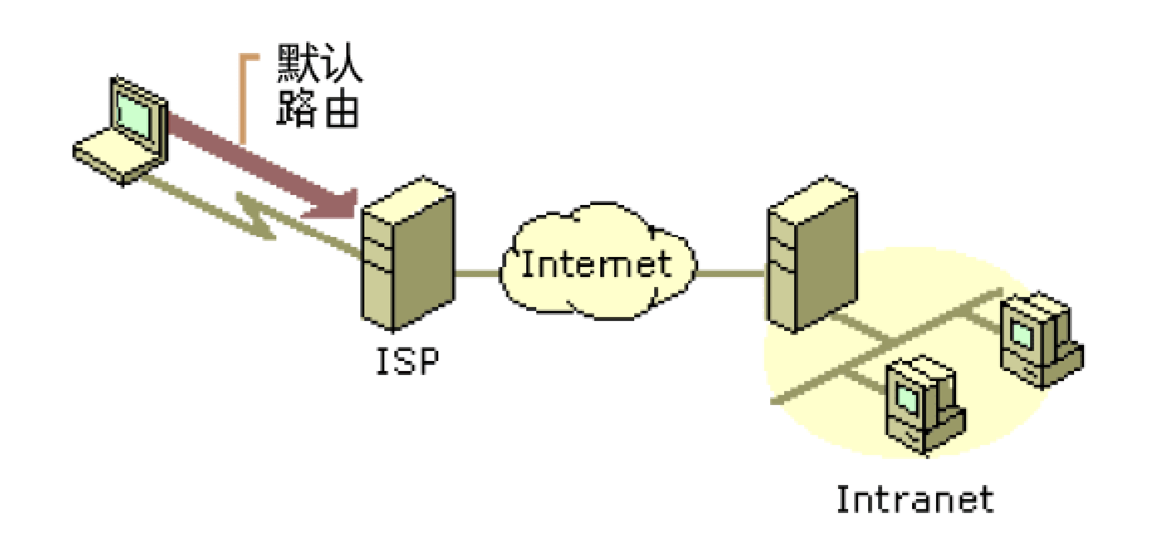


图 8.3　拨打 ISP 时产生一条默认路由

对于绝大多数 VPN 客户机而言，上述机制并不会造成困扰，因为通常 VPN 客户机在

某一时刻或者与 Intranet 进行数据通信或者与 Internet 进行数据通信，而不会同时与两者进行通信。

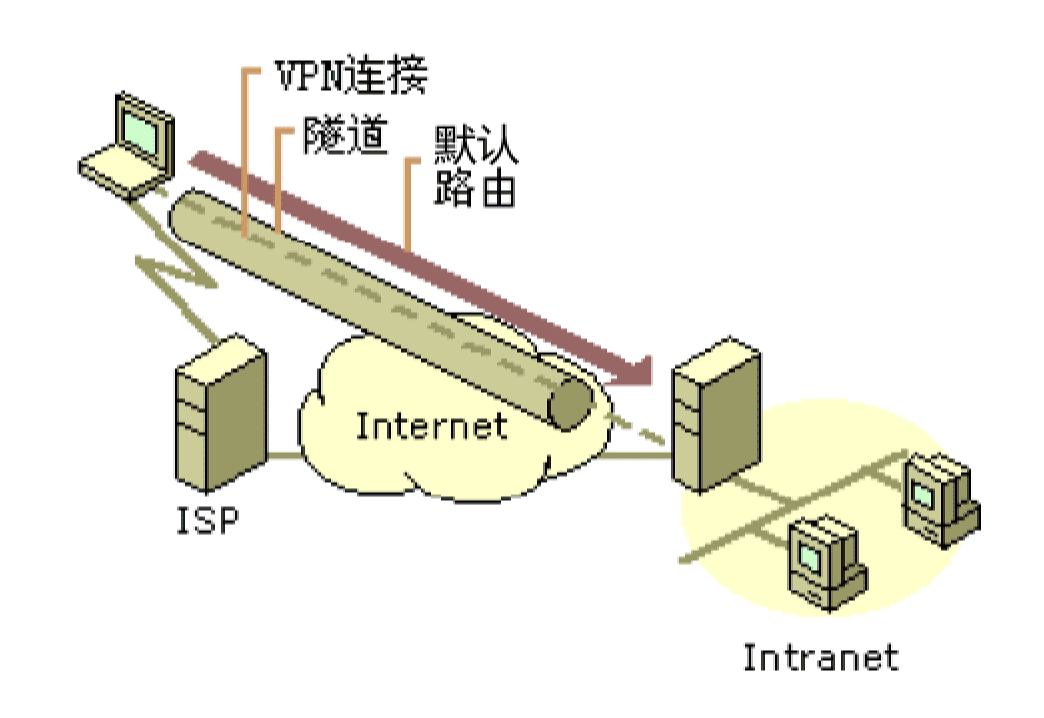


图 8.4　VPN 连接创建时产生另一条新默认路由

2. 路由器-路由器 VPN 连接

1)　临时路由器-路由器的 VPN 连接和永久路由器-路由器 VPN 连接

路由器-路由器 VPN 连接既可以是临时性的，也可以是永久性的。

临时路由器-路由器的 VPN 连接只有当有数据包需要经过 VPN 按需拨号接口(Demand-dial Interface)转发时才被建立起来，在过了一段特定长度空闲时间后即被断开。VPN 客户机(主叫路由器)和 VPN 服务器(被叫路由器)均需配置空闲时间长度。VPN 客户机按需拨号接口的默认空闲时间没有限制，而 VPN 服务器的默认空闲时间为 20min。

永久路由器-路由器 VPN 连接，只要路由器开始启动，即可建立。在永久路由器-路由器的 VPN 连接中，无论是否有数据流发送，连接始终保持，即便连接被中断，也会自动尝试再次恢复连接。

2)　使用拨号 ISP 连接的 VPN

如果 VPN 服务器和 VPN 客户机双方均通过诸如 T1 或帧中继等永久性 WAN 链路与 Internet 直接相连，则该 VPN 连接可以是永久性的，且全天候可用。然而，如果没有可用的永久性 WAN 链路，则可以选择使用拨号 ISP 配置一个随需(On-demand)路由器-路由器 VPN 连接。

在通常 VPN 实现中，远程分部办公室路由器接收到需要转发的数据流时，会自动建立一条随需路由器-路由器 VPN 连接。例如某远程分部办公室路由器接收到需要发往公司总部的数据包时，首先使用拨号链路与本地 ISP 取得连接；当可用的 Internet 连接建立起来后，该分部路由器-VPN 客户机，即可创建一条路由器-路由器 VPN 连接，与公司总部路由器-VPN 服务器相连。

3)　静态路由和动态路由

在按需拨号接口被建立起来，且已经确定是临时连接还是永久连接之后，就可以选用以下 3 种方法之一在路由表中添加路由信息。

(1)　对于临时连接，可以通过手工方式添加路由信息。手工配置静态路由信息适用于路由器数目不多的小型应用方案中。

(2)　对于永久连接，可以使用“自动静态更新”(Auto-Static Updates)来对静态路由做周期性更新。自动静态路由可适用于有大量路由信息的较大的应用环境中。



(3) 对于永久连接，则可以将 VPN 连接看作一条点对点链路，选用其他合适的路由协议，对路由器-路由器 VPN 连接进行动态路由维护。

VPN 对于服务提供商和公司企业来说，都蕴含着极大的商机。业界分析家已意识到了 VPN 将带给服务提供商的极大利润。国外 3Com、Cisco、Shiva、Ascend 等厂商已纷纷推出各自的 VPN 产品，急于抢占 VPN 市场。中国的 VPN 市场也开始启动，据悉，中国电信、ISP 均考虑开拓 VPN 业务。虽然目前国内企业计划利用 VPN 的还不多，但相信随着企业对 VPN 认识的深入、市场竞争的加剧、分支机构范围的扩大，构建 VPN 的国内企业将越来越多。

当然，目前 VPN 还存在一些缺陷。VPN 协议还未完全标准化而各 VPN 产品厂商对 VPN 的认识也不尽相同，产品之间的互通性还有待解决；ISP 无法跨越自己的骨干网保证 QoS，SLA(服务水平协议)只能对 ISP 运营管理的网段起作用，对于跨国企业而言，全球 IP VPN 仍有赖于未来漫游技术及更先进的 IP 账务系统发展与普及方能实现。

8.2 网络地址转换 NAT

8.2.1 NAT 概述

下面讨论另一种情况，就是在专用网内部的一些主机本来已经分配到了本地 IP 地址，但现在又想和 Internet 上的主机通信(并不需要加密)，应当采取什么措施呢？

最简单的办法就是设法再申请一些全球 IP 地址。但这在很多情况下是不容易做到的，因为全球 IP 地址已所剩不多了。目前使用最多的方法是采用网络地址转换。

网络地址转换(Network Address Translation，NAT)方法是在 1994 年提出的。这种方法需要在专用网连接到 Internet 的路由器上安装 NAT 软件。装有 NAT 软件的路由器叫作 NAT 路由器，它至少有一个有效的内部全球地址 IPG。这样，所有使用本地地址的主机和外界通信时都要在 NAT 路由器上将其本地地址转换成 IPG 才能和 Internet 连接。NAT 属接入广域网(WAN)技术，是一种将私有(保留)地址转化为合法 IP 地址的转换技术，它被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。原因很简单，NAT 不仅完美地解决了 IP 地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。

8.2.2 NAT 的两种实现模式

NAT 技术中最常用的实现模式有两种，即静态 NAT 和动态 NAT。

静态 NAT 是建立内部本地地址和内部全球地址的一对一的永久映射。当外部网络需要通过固定的全局可路由地址访问内部主机时，静态 NAT 就显得十分重要。

动态 NAT 是建立内部本地地址和内部全球地址池的临时对应关系，如果经过一段时间，内部本地地址没有向外的请求或者数据流，该对应关系将被删除。

如图 8.5 所示，内部主机 X 用本地地址 IPX(10.1.0.1)和 Internet 上主机 Y(194.4.5.6)通信的详细过程如下。

(1) 内部主机 X(10.1.0.1)发起对 IPY(194.4.5.6)的连接。

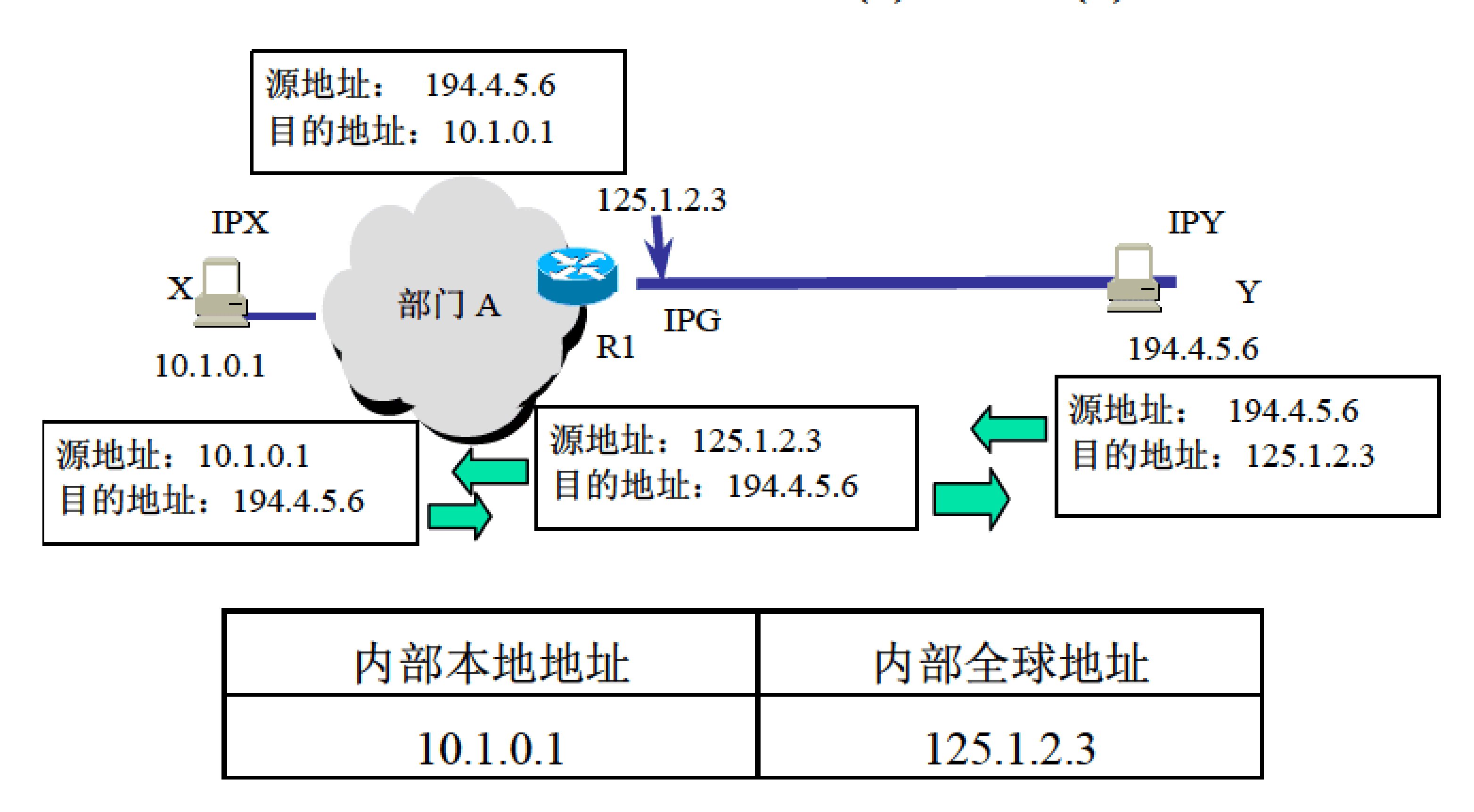
(2)　所发送的数据报经过 NAT 路由器。当 NAT 路由器收到以 IPX(10.1.0.1)为源地址的第一个数据包时，引起路由器检查 NAT 映射表。该地址配置有静态映射，就执行第(3)步；如果没有静态映射，就进行动态映射，路由器从内部全局地址池中选择一个有效的地址，并在 NAT 映射表中创建 NAT 转换记录。这种记录叫基本记录。

(3)　路由器用 10.1.0.1 对应的 NAT 转换记录中的全局地址替换数据包源地址，转换成全球地址 IPG(125.1.2.3)，但目的地址 IPY(194.4.5.6)保持不变，然后发送到 Internet。

(4)　目的地址 IPY(194.4.5.6)收到数据包后，向 IPG(125.1.2.3)发回响应包。

(5)　NAT 路由器收到主机 Y 发回的数据包时，知道数据包中的源地址是 IPY(194.4.5.6)，目的地址是 IPG(125.1.2.3)。根据 NAT 转换表，NAT 路由器将目的地址 IPG(125.1.2.3)转换为 IPX(10.1.0.1)，转发给最终的内部主机 X。

(6)　主机 X 收到应答包，并继续保持会话。第(1)步到第(5)反复执行，直到会话结束。



内部本地地址	内部全球地址
10.1.0.1	125.1.2.3

图 8.5　NAT 转换过程

如果 NAT 路由器具有多个全球 IP 地址，就可以同时将多个本地地址转换为全球 IP 地址，因而使多个拥有本地地址的主机能够和 Internet 上的主机进行通信。

还有一种 NAT 转换表将传输层的端口号也利用上，这样就可以用一个全球 IP 地址使多个拥有本地地址的主机同时和 Internet 上的不同主机进行通信，这种方法叫作网络地址端口转换(Network Address Port Translation，NAPT)，它将内部地址映射到外部网络的一个 IP 地址的不同端口上。

NAPT 普遍应用于接入设备中，它可以将中小型的网络隐藏在一个合法的 IP 地址后面。NAPT 与动态地址 NAT 不仅将内部连接映射到外部网络中的一个单独的 IP 地址上，同时在该地址上加上一个由 NAT 设备选定的 TCP 端口号。

在 Internet 中使用 NAPT 时，所有不同的 TCP 和 UDP 信息流看起来好像来源于同一个 IP 地址。这个优点在小型办公室内非常实用，通过从 ISP 处申请一个 IP 地址，可能将多个连接通过 NAPT 接入 Internet。

图 8.6 反映了内部源地址 NAPT 的整个映射过程。

(1)　内部主机 192.168.1.5 发起一个到外部主机 63.5.8.10 的连接。

(2)　当路由器接收到 192.168.1.5 为源地址的第一个数据包时，引起路由器检查 NAT 映射表。如果 NAT 没有转换记录，路由器就为 192.168.1.5 作地址转换，并创建一条转换记录。如果启用了 NAPT，就进行另一次转换，路由器将复用全球地址并保存足够的信息，



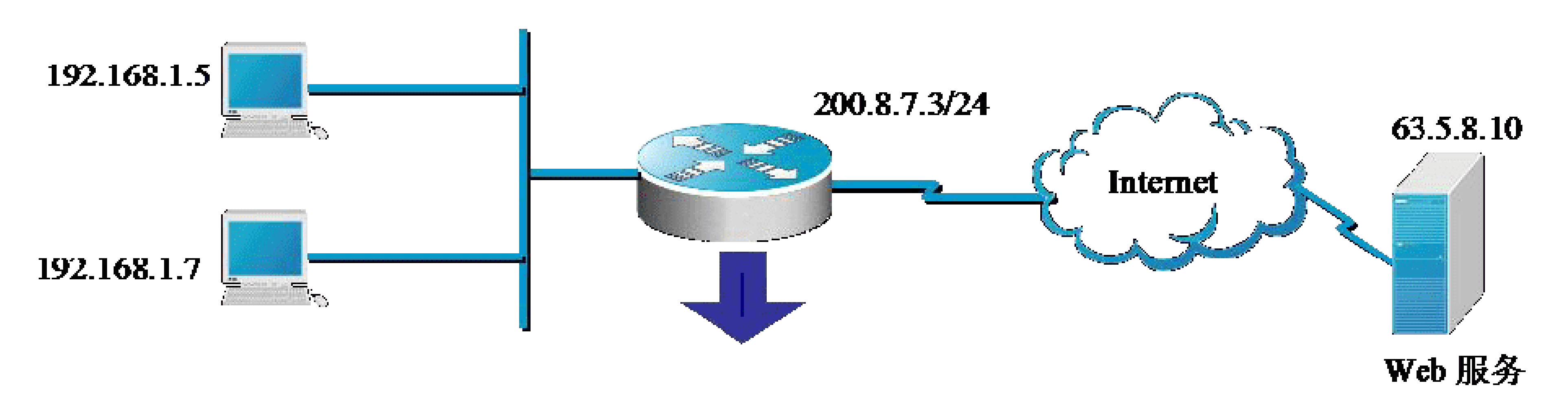
以便还能将全球地址转换回本地地址。NAPT 的地址转换记录称为扩展记录。

(3) 路由器用 200.8.7.3 对应的 NAT 转换记录中的全球地址替换数据包源地址，经过转换后，数据包的源地址变为 200.8.7.3，然后转发该数据包。

(4) 63.5.8.10 主机接收到数据包后，就向 200.8.7.3 发响应包。

(5) 当路由器接收到内部全球地址的数据包时，将以内部全球地址 200.8.7.3 及其端口号、外部全球地址及其端口号为关键字查找 NAT 记录表，将数据包的目的地址转换成 192.168.1.5 并转发给 192.168.1.5。

(6) 192.168.1.5 接收到应答包，并继续保持会话。第(1)步到第(5)步一直重复，直到会话结束。



内部本地地址：端口	内部全球地址:端口	外部全球地址:端口
192.168.1.7:1024	200.8.7.3:1024	63.5.8.10：80
192.168.1.5:1136	200.8.7.3:1136	63.5.8.10：80

图 8.6 内部源地址 NAPT 映射过程

8.3 因特网的网络层安全协议族(IPSec)

8.3.1 IPSec 与安全关联(SA)

1998 年 11 月公布了因特网网络层安全的系列 RFC[RFC 240 1～1411][W-IPSec]。其中最重要的就是描述 IP 安全体系结构的[RFC 2401]和提供 IPSec 协议族概述的[RFC 2411]。IPSec 就是“IP 安全(Security)协议”的缩写。

网络层保密是指所有在 IP 数据报中的数据都是加密的。此外，网络层还应提供源站鉴别(Source Authentication)，即当目的站收到 IP 数据报时，能确信这是从该数据报的源 IP 地址的主机发来的。在 IPSec 中最主要的两个部分是：鉴别首部(Authentication Header，AH)和封装安全有效载荷(Encapsulation Security Payload，ESP)。AH 提供源站鉴别和数据完整性，但不能保密。而 ESP 比 AH 复杂得多，它提供源站鉴别、数据完整性和保密。

在使用 AH 或 ESP 之前，先要从源主机到目的主机建立一条网络层的逻辑连接。此逻辑连接叫作安全关联(Security Association，SA)。这样，IPSec 就将传统的因特网无连接的网络层转换为具有逻辑连接的层。安全关联是一个单向连接。如进行双向的安全通信则需要建立两个安全关联。一个安全关联 SA 由一个三元组唯一地确定，它包括：

(1) 安全协议(使用 AH 或 ESP)的标识符。

(2) 此单向连接的目的 IP 地址。

(3) 一个 32 bit 的连接标识符，称为安全参数索引(Security Parameter Index，SPI)。

对于一个给定的安全关联 SA，每一个 IPSec 数据报都有一个存放 SPI 的字段。通过此 SA 的所有数据报都使用同样的 SPI 值。

8.3.2　鉴别首部(AH)

鉴别首部(AH)插在原数据报数据部分的前面，并将 IP 首部的协议字段置为 51，见图 8.7。在传输过程中，中间的路由器都不查看 AH 首部。当数据报到达目的站时，目的站主机才处理 AH 字段，以鉴别源主机和检查数据报的完整性[RFC 2402]。

AH 首部具有以下的一些字段。

(1)　下一个首部(8 bit)。标志紧接着本首部的下一个首部的类型(如 TCP 或 UDP)。

(2)　有效载荷长度(8 bit)。即鉴别数据字段的长度，以 32 bit 字为单位。

(3)　安全参数索引 SPI(32 bit)。标志一个安全关联。

(4)　序号(32 bit)。鉴别数据字段的长度，以 32 bit 字为单位。

(5)　保留(16 bit)。为今后用。

(6)　鉴别数据(可变)。为 32 bit 字的整数倍，它包含了经数字签名的报文摘要(对原来的数据报进行报文摘要运算)。因此，可用来鉴别源主机和检查 IP 数据报的完整性。

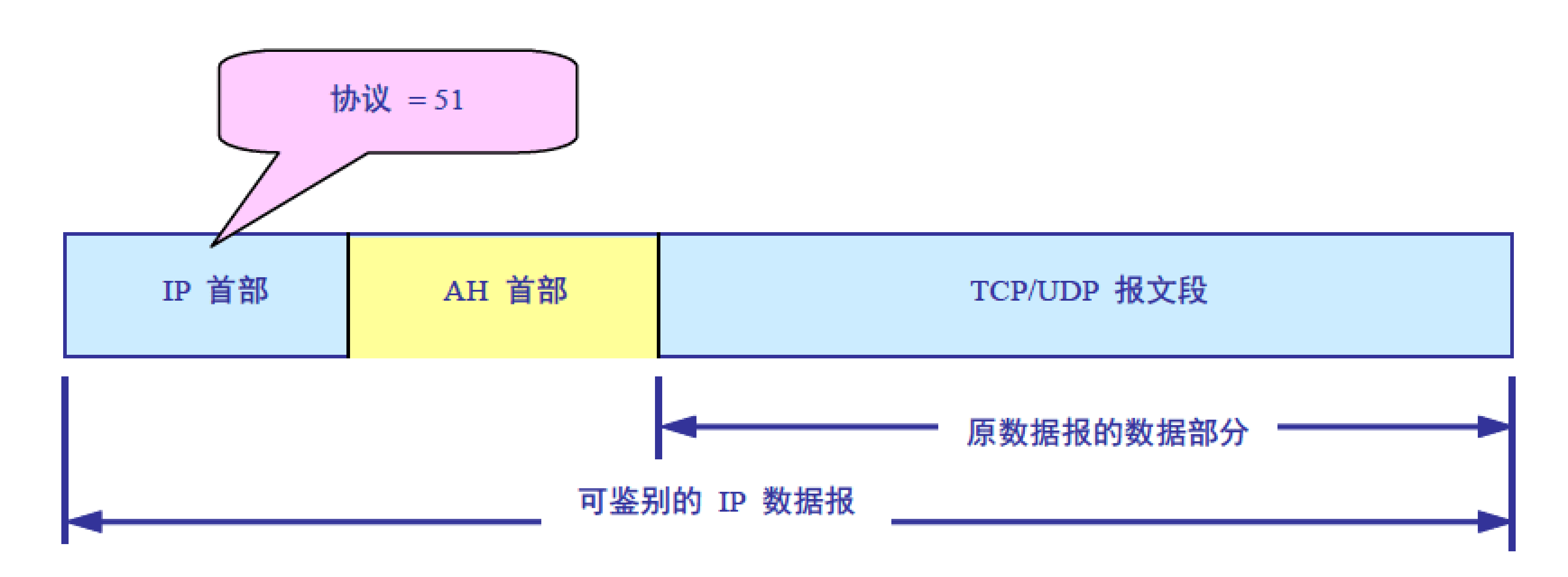


图 8.7　AH 首部的安全数据报中的位置

8.3.3　封装安全有效载荷(ESP)

在 ESP 首部中，有标识一个安全关联的安全参数索引 SPI(32 bit)和序号(32 bit)。在 ESP 尾部中有下一个首部(8 bit，作用和 AH 首部一样)。ESP 尾部和原来数据报的数据部分一起进行加密，见图 8.8，攻击者无法得知所使用的运输层协议。ESP 的鉴别数据和 AH 中的鉴别数据是一样的。因此，用 ESP 封装的数据报既有鉴别源站和检查数据报完整性的功能，又能提供保密。

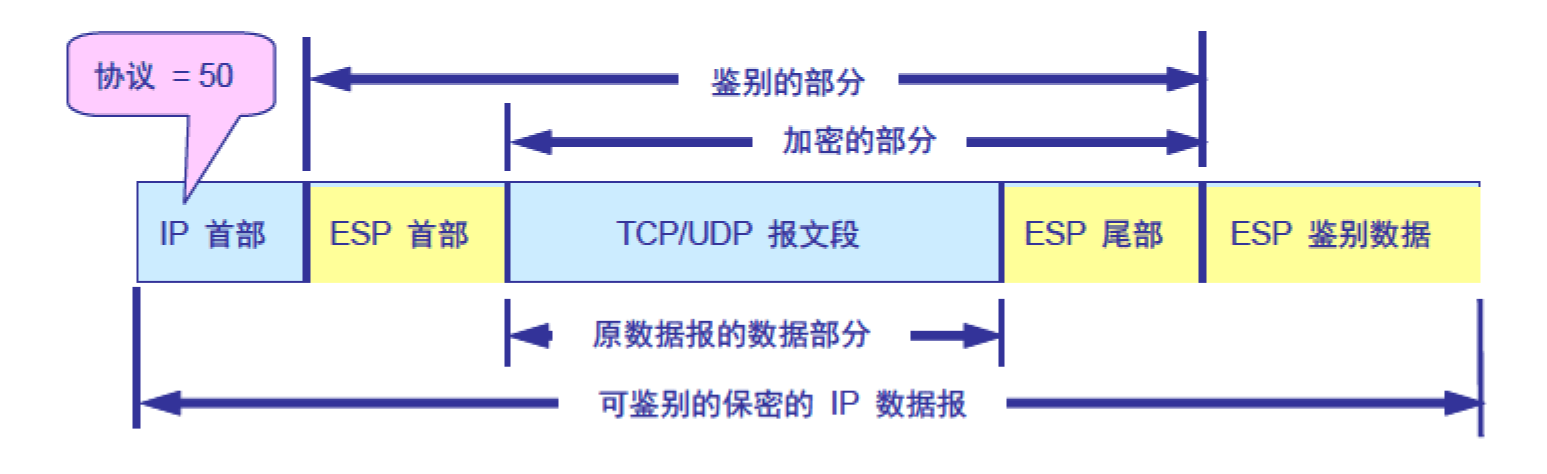


图 8.8　在 IP 数据报中的 ESP 的各字段



8.4　因特网商务中的安全协议

因特网商务就是通过因特网来进行商务活动，如购物、订票、股票交易等。近年来，在商务安全方面较出名的有两个协议，即已在许多因特网交易中使用的安全插口层(Secure Socket Layer，SSL)和有很强竞争潜力的安全电子交易(Secure Electronic Transaction，SET)。

8.4.1　安全插口层(SSL)

SSL 又称为安全套接层，是 Netscape 公司开发的协议，可对万维网客户与服务器之间传送的数据进行加密和鉴别。它在双方的联络阶段协商将使用的加密算法(如用 DES 或 RSA)和密钥，以及客户与服务器之间的鉴别。在联络阶段完成后，所有传送的数据都使用在联络阶段商定的会话密钥。SSL 不仅被所有常用的浏览器和万维网服务器所支持，而且也是运输层安全协议(Transport Layer Security，TLS)的基础[RFC 2246]。

SSL 和 TLS 并不仅限于万维网的应用，它们还可用于 IMAP 邮件存取的鉴别和数据加密。SSL 可看成是在应用层和运输层之间的一个层，见图 8.9。在发送方，SSL 接收应用层的数据(如 HTTP 或 IMAP 报文)，对数据进行加密，然后将加了密的数据送往 TCP 插口。在接收方，SSL 从 TCP 插口读取数据，解密后将数据交给应用层。

SSL 提供以下 3 个功能。

(1)　SSL 服务器鉴别。允许用户证实服务器的身份。具有 SSL 功能的浏览器维持一个表，上面有一些可信赖的认证中心(Certificate Authority，CA)和它们的公开密钥。当浏览器要和一个具有 SSL 功能的服务器进行商务活动时，浏览器就从服务器得到含有服务器的公开密钥的证书。此证书是由某个认证中心 CA 发出的(此 CA 在客户的表中)。这就使得客户在提交其信用卡之前能够鉴别服务器的身份。

(2)　加密的 SSL 会话。客户和服务器交互的所有数据都在发送方加密，在接收方解密。SSL 还有检测攻击者有无窃听传送数据的功能。

(3)　SSL 客户鉴别。允许服务器证实客户的身份。这个信息对服务器是很重要的。例如，当银行将保密的有关财务信息发送给某顾客时，就必须检验接收者的身份。

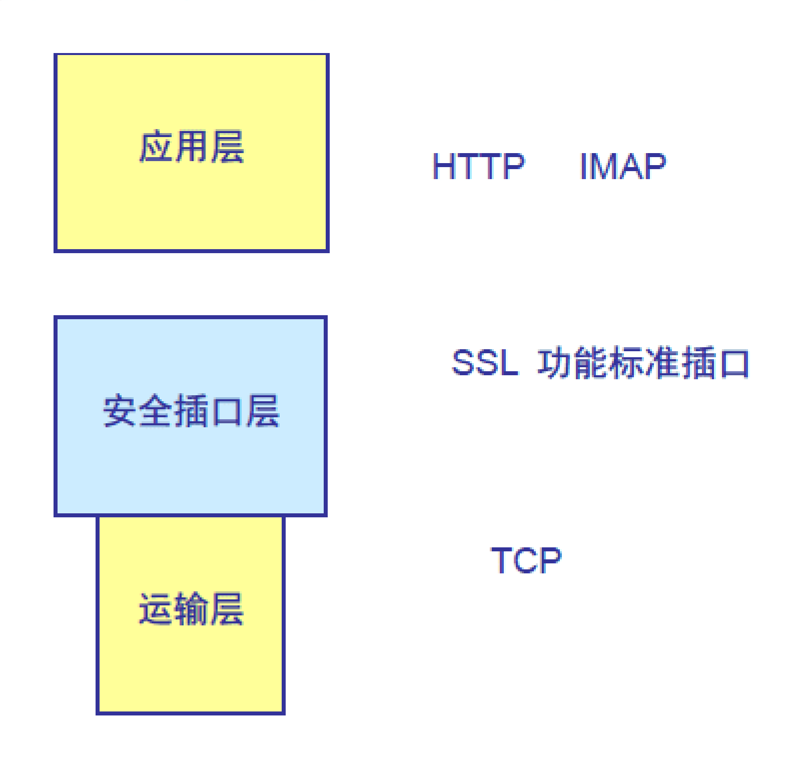


图 8.9　安全插口层(SSL)的位置

下面通过一个简单的例子说明 SSL 的工作原理。

假定 A 有一个使用 SSL 的安全网页。B 上网时用鼠标点击到这个安全网页的链接(这

种安全网页的 URL 的协议部分不是 HTTP 而是 HTTPS)。接着，服务器和浏览器就执行握手协议，其主要过程如下。

(1) 浏览器向服务器发送浏览器的 SSL 版本号和密码编码的参数选择(Preference)(因为浏览器和服务器要协商使用哪一种对称密钥算法)。

(2) 服务器向浏览器发送服务器的 SSL 版本号、密码编码的参数选择及服务器的证书。证书包括服务器的 RSA 公开密钥。此证书用某个认证中心的私有密钥加密。

(3) 浏览器有一个可信赖的 CA 表，表中有每一个 CA 的公开密钥。当浏览器收到服务器发来的证书时，就检查此证书是否在自己的可信赖的 CA 表中。如不在，则后面的加密和鉴别连接就不能再进行下去。如在，浏览器就使用 CA 的公开密钥对证书解密，这样就得到了服务器的公开密钥。

(4) 浏览器随机地产生一个对称会话密钥，并用服务器的公开密钥加密，然后将加密的会话密钥发送给服务器。

(5) 浏览器向服务器发送一个报文，说明以后浏览器将使用此会话密钥进行加密。然后浏览器再向服务器发送一个单独的加密报文，表明浏览器端的握手过程已经完成。

(6) 服务器也向浏览器发送一个报文，说明以后服务器将使用此会话密钥进行加密。然后服务器再向浏览器发送一个单独的加密报文，表明服务器端的握手过程已经完成。

(7) SSL 的握手过程至此已经完成，下面就可开始 SSL 的会话过程。浏览器和服务器都使用这个会话密钥对所发送的报文进行加密。

由于 SSL 简单且开发得较早，因此目前在因特网商务中使用比较广泛。但 SSL 并非专门为信用卡交易而设计的，它只是在客户与服务器之间提供了一般的安全通信。SSL 还缺少一些措施以防止在因特网商务中出现各种可能的欺骗行为。

8.4.2　安全电子交易(SET)

安全电子交易(SET)是专为在因特网上进行安全信用卡交易的协议。它最初是由两个著名信用卡公司 Visa 和 MasterCard 于 1996 年开发的，世界上许多具有领先技术的公司也参与其中。1997 年年底成立了实体 SETCo，目的是在全球推广使用 SET。

SET 的主要特点如下。

(1) SET 是专为与支付有关的报文进行加密的，它不能像 SSL 那样对任意的数据(如正文或图像)进行加密。

(2) SET 协议涉及 3 方，即顾客、商家和商业银行。所有在这 3 方之间交互的敏感信息都被加密。

(3) SET 要求 3 方都有证书。在 SET 交易中，商家看不见顾客传送给商业银行的信用卡号码。这是 SET 的一个最关键的特性。

在一个 SET 交易中要使用 3 个软件。

(1) 浏览器钱包。这个软件集成在浏览器中，它为顾客在购物时提供信用卡和证书的存储和管理的地方，并响应从商家发来的 SET 报文，提示顾客选择信用卡进行支付。

(2) 商家服务器。这是在万维网上提供商品交易的实现引擎。它处理持卡人的交易，并与商业银行通信。

(3) 支付网关(Acquirer Gateway)。这是商业银行使用的软件，处理信用卡的交易，包



括授权和支付，是个相当复杂的软件。

下面以顾客 B 到公司 A 用 SET 购买物品为例来说明 SET 的工作原理。这里涉及两个银行，即 A 的银行(公司 A 的支付银行)和 B 的银行(给 B 发出信用卡的银行)。

(1) B 告诉 A 他想用信用卡购买公司 A 的物品。

(2) A 将物品清单和一个唯一的交易标识符发送给 B。

(3) A 将其商家的证书包括商家的公开密钥发送给 B。A 还向 B 发送其银行的证书，包括银行的公开密钥。这两个证书都用一个认证中心 CA 的私有密钥进行加密。

(4) B 使用认证中心 CA 的公开密钥对这两个证书解密。于是 B 有了 A 的公开密钥和 A 的银行的公开密钥。

(5) B 生成两个数据包：给 A 用的订货信息 OI(Order Information)和给 A 的银行用的购买指令 PI(Purchase Instruction)。OI 包括交易标识符和将要使用的信用卡的类别，但不包含 B 的信用卡号码。PI 则包括交易标识符、B 的信用卡号码以及 B 同意向 A 付出的款数。OI 用 A 的公开密钥加密，而 PI 用 A 的银行的公开密钥加密。B 将加密后的 OI 和 PI 发送给 A。请注意，PI 虽然是给 A 的银行用的，但并不是由 B 直接发送给 A 的银行。

(6) A 生成对信用卡支付请求(Payment Request)的授权请求(Authorization Request)，它包括交易标识符。

(7) A 用银行的公开密钥将一个报文加密发送给银行，此报文包括授权请求、从 B 发过来的 PI 数据包及 A 的证书。

(8) A 的银行收到此报文，将其解密。A 的银行要检查此报文有无被篡改，以及检查在授权请求中的交易标识符是否与 B 的 PI 数据包给出的一致。

(9) A 的银行通过传统的银行信用卡信道向 B 的银行发送请求支付授权的报文。

(10) B 的银行准许支付后，A 的银行就向 A 发送加密的响应。此响应包括交易标识符。

(11) 若此次交易被批准，A 就向 B 发送响应报文。此报文作为收据，并通知 B：“支付已被接受，所购物品即将发出”。

SET 的特点中很重要的一点就是购物人的信用卡号码不向商家暴露。我们注意到在上面的第(5)项中，B 使用银行的密钥对其信用卡号码加密。

8.5 PGP 协议

PGP(Pretty Good Privacy，更好的保护隐私)是一个基于 RSA 公匙加密体系的邮件加密软件。可以用它对邮件保密以防止非授权者阅读，它还能对邮件加上数字签名，从而使收信人可以确认邮件的发送者，并能确信邮件没有被篡改。它可以提供一种安全的通信方式，而事先并不需要任何保密的渠道用来传递密匙。它采用了一种 RSA 和传统加密的杂合算法，用于数字签名的邮件文摘算法和加密前压缩等，还有一个良好的人机工程设计。它的功能强大，有很快的速度，而且它的源代码是免费的。

8.5.1 功能

PGP 使用加密及校验的方式，提供了多种功能和工具，帮助保证电子邮件、文件、磁盘以及网络通信的安全。可以使用 PGP 做以下这些事情：

(1) 在任何软件中进行加密/签名及解密/校验。通过 PGP 选项和电子邮件插件，可以在任何软件中使用 PGP 的功能。

(2) 创建及管理密钥。使用 PGPkeys 来创建、查看和维护 PGP 密钥对以及把任何人的公钥加入公钥库中。

(3) 创建自解密压缩文档(Self-Decrypting Archives, SDA)。可以建立一个自动解密的可执行文件。任何人不需要事先安装 PGP，只要得知该文件的加密密码，就可以把这个文件解密。这个功能尤其在需要把文件发送给没有安装 PGP 的人时特别好用。并且，此功能还能对内嵌其中的文件进行压缩，压缩率与 ZIP 相似，比 RAR 略低(某些时候略高，比如含有大量文本)。

(4) 创建 PGPdisk 加密文件。该功能可以创建一个.pgd 的文件，此文件用 PGP Disk 功能加载后，将以新分区的形式出现，可以在此分区内放入需要保密的任何文件。其使用私钥和密码两者共用的方式保存加密数据，保密性坚不可摧，但需要注意的是，一定要在重装系统前记得备份“我的文档”中的 PGP 文件夹里的所有文件，以备重装后恢复私钥，否则将永远没有可能再次打开曾经在该系统下创建的任何加密文件。

(5) 永久的粉碎销毁文件、文件夹，并释放出磁盘空间。可以使用 PGP 粉碎工具来永久地删除那些敏感的文件和文件夹，而不会遗留任何数据片段在硬盘上。也可以使用 PGP 自由空间粉碎器来再次清除已经被删除的文件实际占用的硬盘空间。这两个工具都是要确保用户所删除的数据将永远不可能被别有用心的人恢复。

(6) 全盘加密，也称完整磁盘加密。该功能可将整个硬盘上所有数据加密，甚至包括操作系统本身。提供极高的安全性，没有密码的人绝无可能使用您的系统或查看硬盘里存放的文件、文件夹等数据。即便是硬盘被拆卸到另外的计算机上，该功能仍将忠实地保护数据、加密后的数据维持原有的结构，文件和文件夹的位置都不会改变。

(7) 即时消息工具加密。该功能可将支持的即时消息工具(IM，也称即时通信工具、聊天工具)所发送的信息完全经由 PGP 处理，只有拥有对应私钥的和密码的对方才可以解开消息的内容。任何人截获到也没有任何意义，仅仅是一堆乱码。

(8) PGP zip，PGP 压缩包。该功能可以创建类似其他压缩软件打包压缩后的文件包，但不同的是其拥有坚不可摧的安全性。

(9) 网络共享。可以使用 PGP 接管共享文件夹本身及其中的文件，安全性远远高于操作系统本身提供的账号验证功能。并且可以方便地管理允许的授权用户可以进行的操作。极大地方便了需要经常在内部网络中共享文件的企业用户，免于受蠕虫病毒和黑客的侵袭。

(10) 创建可移动加密介质(USB/CD/DVD)产品。

8.5.2 电子邮件加密

寄出的电子邮件内容会不会被人窃取，会不会收到伪冒的电子邮件，PGP 可以自动地帮做 eMail 加密及签章。

可以自己设定各种安全政策，如收件人是谁、主旨内容为何时就需要加密与签章，其他情况可以只签章(证明这信是本人发的)而不加密；只要选中 PGP Mail Proxy Service 复选框，PGP 就依照设定的规则自动执行，PGP 会找出收件人的公钥，使用此公钥来加密邮件内容，再用自己的私钥来签章该邮件；对方 PGP 收到该邮件时，会先用你的公钥来验证该



邮件确是你寄出的，然后用他自己的私钥来解开该邮件内容。所有动作都由 PGP 在背后自动执行。

也可以不用 PGP Mail Proxy Service，自己可以先用 Notepad 之类的工具编写邮件内文，然后按 PGP Icon 选择 Current Window，再选择 Encrypt & Sign 或 Encrypt，就会出现计算机里所有公钥的人让人选择，可以选取多个人，这些人就是可以解密你加密的内容。

如果只是要附件文件加密，如一张自拍照(图档)或是研发中的 CAD/CAM 文档，或是一般机密的 Office 档案，可以直接在档案总管下右击，在弹出的快捷菜单下选择 PGP Desktop 命令，然后选择 Secure … with key…，PGP 窗口弹出选择可解开此加密文档的人(金钥)，该档案就被加密。

8.5.3 虚拟磁盘驱动器

如果只是想要加密计算机里的私密数据，除了本人(或加上指定的人)没有其他人可以解密这些数据。所以即使计算机遗失、计算机被盗用、甚或检调单位来搜，也不用担心这些私密资料外泄。通常，最安全的方法伴随的是使用不便，但是 PGP 的虚拟磁盘驱动器加密功能既安全又好用。

可以指定硬盘某空间来做加密磁盘驱动器，在这磁盘驱动器里的档案及数据都是加密过的，只有自己或是被指定可出示私钥或使用者代号密码才能解密这些数据。任何机密的档案都可以放到里面，加过密的磁盘的操作如同一般档案总管，依旧使用 Word、Excel、Photoshop 等软件包或应用程序来打开它，完全不受影响，因为 PGP 自动处理进出这磁盘驱动器的加解密工作。

电子邮件软件如 Outlook、Outlook Express 等，无论是收件箱还是寄件备份，其实都是档案而已，如 Outlook 是.pst 文件，这些电子邮件档案通常包括很多机密内容。

8.5.4 加密与压缩功能

如果只是想将部分目录或档案加密后传给别人(eMail 或 FTP 等)，当然可以用 WinZip 或 WinRAR 等工具里的密码保护，但其加密算法较弱，同时密码也可能被猜到，这对于要传送极机密的档案数据是有风险的。PGP 则提供较高安全的类似工具，如果对方有 PGP，应该使用对方的公钥来加密，如果要将加密文档送给多人，就加入多个公钥，拥有任何一个公钥所对应的私钥都可以解密这些文档，这是使用 RSA 2048 bit 加密算法(内定)，所以比较安全；加完密后再用自己的私钥来签章，PGP 同时帮助将文档压缩。

如果对方没有 PGP 时，可以使用 Self-Decrypting Archive(SDA)，PGP 会要求输入加密密码，然后使用该密码来加密文档，并产生可自动解密的执行文档，当然，必须另外告知对方解密的密码。

习题与思考题八

1. VPN 的优越性有哪些？
2. VPN 主要采用了哪几项技术？

3. NAT 网络地址转换的目的是什么？静态 NAT 和动态 NAT 有何区别？

4. 请举例说明 NAT 网络地址转换的工作过程。

5. 某一办公室有两台计算机需要同时连接 Internet，只有一台 ADSL，一个账号且不能共享，请给出两种实现方案，说明实现方法并画出示意图。

6. 虚拟专用网的含义是什么？

7. 在网络地址转换(NAT)中，内部主机 X(本地地址 IPX)要和外部因特网上的主机 Y(全球地址 IPY)进行通信，NAT 路由器的全球地址 IPG:

(1) NAT 路由器收到 X 发出报文时，如何将地址进行变换？

(2) NAT 路由器收到 Y 发回报文时，如何将地址进行变换？

8. 简述 IPSec 的主要特点。

9. 简述安全插口层 SSL 的主要特点。

10. 简述 PGP 协议的主要功能。

第 9 章　计算机网络管理与维护技术

学习目标

对于一个庞大的计算机网络来说，良好的管理与维护是保证网络正常运转的必要条件，这就要求网络管理人员掌握一定的管理与维护技术。系统学习 Windows 自带的常用网络工具，网卡、集线器、交换机、路由器、网线和 RJ-45 接头等网络连接设备的维护，网络的性能优化，常用网络故障及排除方法。通过本章的学习，读者应该掌握以下内容：

- 掌握网络管理的基本概念、网络管理协议、网络管理工具、网络维护方法。
- 掌握 Windows 自带的一些网络工具的使用方法，网络连接设备的维护方法和技巧，内存、CPU、硬盘和网络接口的优化方法，Internet 常见故障分析和排除方法，局域网常见故障分析和排除方法。
- 了解网络常见故障排除的思路和工具。

9.1　网络管理技术

网络管理包括对硬件、软件和人力的使用、综合与协调，以便对网络资源进行监视、测试、配置、分析、评价和控制，这样就能以合理的价格满足网络的一些需求，如实时运行性能、服务质量等。网络管理常简称为网管。

网络管理是指网络管理员通过网络管理程序对网络上的资源进行集中化管理的操作，包括配置管理、性能和记账管理、问题管理、操作管理和变化管理等。一台设备所支持的管理程度反映了该设备的可管理性及可操作性。

而交换机的管理功能是指交换机如何控制用户访问交换机，以及用户对交换机的可视程度如何。通常，交换机厂商都提供管理软件或满足第三方管理软件远程管理交换机。一般的交换机满足 SNMP MIB I / MIB II 统计管理功能。而复杂一些的交换机会增加通过内置 RMON 组(mini-RMON)来支持 RMON 主动监视功能。有的交换机还允许外接 RMON 探头监视可选端口的网络状况。

9.1.1　网络管理的意义

随着计算机网络的发展与普及，一方面，对于如何保证网络的安全、组织网络高效运行提出了迫切的要求；另一方面，计算机网络日益庞大，使管理更加复杂。这主要表现在以下几个方面。

(1)　网络覆盖范围越来越大。

(2)　网络用户数目不断增加。

(3)　网络共享数据量剧增。

(4)　网络通信量剧增。

(5)　网络应用软件类型不断增加。



(6)　网络对不同操作系统的兼容性要求不断提高。

这种大型、复杂、异构型的网络靠人工是无法管理的，随着网络管理技术的日益成熟，网络管理显得越来越重要。计算机网络管理技术的发展是与 Internet 的发展同步进行的，随着网络技术的发展，网络管理技术也得到了迅速的发展。时至今日，计算机时代和全球信息化已经到来，网络管理和网络安全等问题的重要性日益突出。一旦计算机网络崩溃，将会给企业、公司、单位网络中的各种数据和信息资源，以及人们的工作、学习和日常生活带来巨大的损失。因此，网络管理成为网络技术发展中的一项重要技术，它不但对网络技术的发展有着重要的影响，也是现代信息网络中最重要的研究课题之一，并为越来越多的人所重视。自 20 世纪 80 年代起，随着一系列网络管理标准的出台，出现了大量的商用网络管理系统。

随着网络规模的扩大，网络已不再是单一型的网络，而是由若干个大大小小的子网组成，同时集成了多种网络操作系统的平台，包括各种不同厂家、公司的网络设备和产品。此外，为了提供各种服务，还集成了多种网络软件。因而，如果没有一个高效的网络管理系统，则很难向网络用户提供正常的网络服务，也很难保障网络能无故障、安全地运行。因此，为了保证计算机网络中硬件设备和软件的正常运行，除了需要专门的网络管理技术人员外，还需要利用专用的网络管理工具来维护和管理网络的运行。

总之，现代化的网络管理技术集通信技术、网络技术、Internet 服务技术和信息处理技术等于一身，而现代化网络的管理人员则应当能够通过网络管理平台和管理工具调度和协调资源的使用，并可以对网络实行配置管理、故障管理、性能管理和安全管理等多方面管理工具的人员。

9.1.2　网络管理的基本概念

1. 网络管理的定义

对于一个网络来说，首先应当建立起网络，实现网络设计的功能。其次是通过网络管理系统保证建立起的网络系统能够持续、正常、稳定、安全和高效地运行。此外，当网络出现故障时，网络管理系统还应当能够进行及时的报告和处理，从而保障网络的正常运行。因此，网络管理就是为了完成上述目标而对网络系统实施的一系列方法的措施，换言之，网络管理就是指通过某种方式对网络状态进行的调整，其目的是使网络能正常、高效地运行，并使网络中的各种资源得到更加高效的利用，当网络出现故障时，系统应能及时地作出报告和处理。

2. 网络管理的分类

网络管理为控制、协调和监控网络资源提供了手段，其实质就是网络管理者与被管理对象之间如何利用网络实现信息交换，最终完成网络管理的功能。

从范围来看，可以将网络管理分为以下两类。

(1)　狭义网络管理。仅指对网络交换量等网络参考性能的管理。

(2)　广义网络管理。是指对网络应用系统的管理。



3. 网络管理系统

1) 网络管理系统的定义

通常网络管理是由网络管理系统来实施的，对一个网络管理系统的定义应当包含以下几项内容。

(1) 系统的功能。一个网络管理系统首先应明确其具有的功能。

(2) 明确网络资源。在网络管理中，对于网络资源的管理占有很大一部分比例。网络资源通常被定义为网络系统的软件、硬件及所提供的网络服务和信息等资源。由此，在网络管理系统中只有明确地表示网络资源，才能对它们实施管理。

(3) 表明网络的管理信息。网络管理系统对网络实施管理时，必须依赖系统中的网络管理信息，因此，在设计网络管理系统时，必须解决以下问题。

- 如何表示用于网络管理的信息？
- 如何传送上述信息？
- 传送信息中使用何种协议？

(4) 确定网络管理信息的结构，即使用什么结构的网络管理系统对网络实现管理。

2) 网络管理系统的基本功能

一个实用的网络管理系统应当包括以下基本的网络管理功能。

(1) 为用户制定、设置和实施系统的授权访问策略。

(2) 为用户制定、设置和实施共享资源的授权访问策略。

(3) 能够收集和监控网络中各种设备和设施的工作参数，并能够依据这些信息进行处理、管理和控制。

4. 网络管理内容

目前国际标准化组织(ISO)在网络管理的标准化上做了许多工作，它特别定义了网络管理的 5 个功能域。

- 配置管理：管理所有的网络设备，包括各设备参数的配置与设备账目的管理。
- 故障管理：找出故障的位置并进行恢复。
- 性能管理：统计网络的使用状况，根据网络的使用情况进行扩充，确定设置的规划。
- 安全管理：限制非法用户窃取或修改网络中的重要数据等。
- 计费管理：记录用户使用网络资源的数据，调整用户使用网络资源的配额和记账收费。

1) 配置管理

配置管理的目的在于随时了解系统网络的拓扑结构及所交换的信息，包括连接前静态设定的和连接后动态更新的。配置管理调用客体管理功能、状态管理功能和关系管理功能。

(1) 客体管理功能。客体管理功能为管理信息系统用户(MIS 用户)提供一系列功能，完成被管理客体的产生、删除报告和属性值改变的报告。

(2) 状态管理功能。

① 通用状态属性：指客体应具有的操作态、使用态和管理态 3 种通用状态属性。

② 状况属性：定义了下列 6 个属性以限制操作态、使用态和管理态，表示应用于资

源的特定条件，包括告警状况属性、过程状况属性、可用性状况属性、控制状况属性、备份状况属性、未知状况属性。

(3) 关系管理功能。管理者需有检查系统不同部件间和不同系统间关系的能力，以确定系统某部分的操作如何依赖于其他部分或如何被依赖。用户需有能力改变部分之间、系统之间以及系统与部件之间的关系，也应有能力得知是何种原因导致这种变化。

2) 故障管理

故障管理的目标是自动监测、记录网络故障并通知用户，以便网络有效地运行。

故障管理包含以下几个步骤：①判断故障症状；②隔离该故障；③修复该故障；④对所有重要子系统的故障进行修复；⑤记录故障的监测及其结果。

3) 性能管理

性能管理的目标是衡量和呈现网络性能的各个方面，使人们可以在一个可接受的水平上维护网络的性能，性能变量的例子有网络吞吐量、用户响应时间和线路利用率。

性能管理包含以下几个步骤。

(1) 收集网络管理者感兴趣的变量的性能参数。

(2) 分析这些数据，以判断是否处于正常水平。

(3) 为每个重要的变量决定一个适合的性能阈值，超过该阈值就意味着网络出现故障。

4) 安全管理

安全管理的目标是按照本地的指导来控制对网络资源的访问，以保证网络不被侵害，并保证重要信息不被未授权的用户访问。

安全管理子系统将网络资源分为授权和未授权两大类。它执行以下几种功能。

(1) 标识重要的网络资源。

(2) 确定重要的网络资源和用户集间的映射关系。

(3) 监视对重要网络资源的访问。

(4) 记录对重要网络资源的非法访问。

5) 计费管理

计费管理的目标是衡量网络的利用率，以便一个或一组用户可以按规则利用网络资源，这样的规则使网络故障降低到最小，也可以使所有用户对网络的访问更加公平。

为了达到合理的计费管理目的，首先必须通过性能管理测量出所有重要网络资源的利用率，对其结果的分析使得对当前的应用模式具有更深入的了解，并可以在该点设置定额。对资源利用率的测量可以产生计费信息，并产生可用来估价费率的信息以及可用于资源利用率优化的信息。

5. 网络管理系统的基本模型

公认的网络管理系统基本模型由 4 部分组成，即多个被管代理(Agent)、至少一个网络管理者或称管理工作站、一种通用的网络管理协议(CMIP 或 SNMP)和一个或多个管理信息库(MIB)。网络设备、计算机主机、应用等被称为被管设备，在这些设备上驻留有代理，代理实际上是一个小巧的应用程序。管理者也是一个程序，负责与用户交互，并通过代理对设备进行管理。管理者与代理通过网络管理协议通信。MIB 相当于一个数据库，提供有关被管网络设备的信息。因此，网络管理系统的模型包含以下 4 个基本的逻辑部分。



(1) 管理对象指网络中具体可以操作的参数。

(2) 管理进程(Manager)指对网络中的设备和设施进行全面管理和控制的软件程序。

(3) MIB 指记录网络中各种管理对象的信息库。

(4) 管理协议(CMIP 或 SNMP)用于在管理系统与管理对象之间传递和解释操作命令。

9.1.3 网络管理协议(SNMP)

第一个使用的网络管理(简称网管)协议称为简单网络管理协议(SNMP，又称 SNMP 第一版或 SNMPv1)，SNMP 是由因特网工程任务组(Internet Engineering Task Force，IETF)提出的面向 Internet 的管理协议，当时这个协议被认为是临时的、简单的、解决当时急需解决的问题的协议，而复杂的、功能强大的网络管理协议需要进一步设计。

20 世纪 80 年代，在 SNMP 的基础上设计了两个网络管理协议：一个称为 SNMP 第二版(简称 SNMPv2)，它包含了原有的特性，这些特性目前被广泛使用，同时增加了很多新特性以克服原先 SNMP 的缺陷。另一个称为简单网关监控协议(SGMP)，用来对通信线路进行管理。

SNMP 的管理对象包括网桥、路由器、交换机等内存和处理能力有限的网络互联设备。它采用轮询监控方式，管理者隔一定时间间隔向代理请求管理信息，管理者根据返回的管理信息判断是否有异常事件发生。轮询监控的主要优点是对代理资源的要求不高，缺点是管理通信的开销大。由于 SNMP 的简单性得到了业界广泛的支持，成为目前最流行的网络管理协议。

1. SNMP 网络管理模型

SNMP 模型的体系结构如图 9.1 所示。SNMP 网络管理模型是由以下前 3 个基本部分再加上 SNMP 协议组成的。

1) 管理进程

管理进程是一个或一组软件程序，它一般运行在网络管理站或网络管理中心的主机上。它在 SNMP 协议支持下命令管理代理执行各种管理操作。管理进程的功能是完成各种网络管理功能，通过各种设备中的管理代理实现对网络内的各种设备、设施和资源的控制。另外，管理人员还可以通过管理进程对全网进行管理。管理进程可以通过图形用户接口，以容易操作的方式显示各种网络信息以及网络中各网络代理的配置图等。有时，网络进程也会将各个管理代理中的数据集中存储，以备事后分析。

2) 管理代理

管理代理是一种在被管理的网络设备上运行的软件，负责执行管理进程的管理操作。管理代理直接操作本地的信息库 MIB，还可以根据要求改变本地信息库或将数据直接传送给管理进程。管理代理具有两个基本的管理功能。

(1) 读取 MIB 中各种变量的值，这里的变量就是管理对象。

(2) 修改 MIB 中各种变量的值。

3) MIB

MIB 管理信息库记录管理对象的各种信息。它是一个概念上的数据库，由各个管理对象组成，每个管理代理管理 MIB 中属于本地的管理对象，各管理代理控制的管理对象共同

构成全网的管理信息库。

4)　管理协议

用于在管理系统与管理对象之间传递和解释管理操作命令的 SNMP 协议。许多网络管理软件要求所管理的设备支持 SNMP 协议，如果不支持，则无法使用该软件实现对网络系统设备的自动识别和管理功能，如 HP 公司的 OpenView 软件。

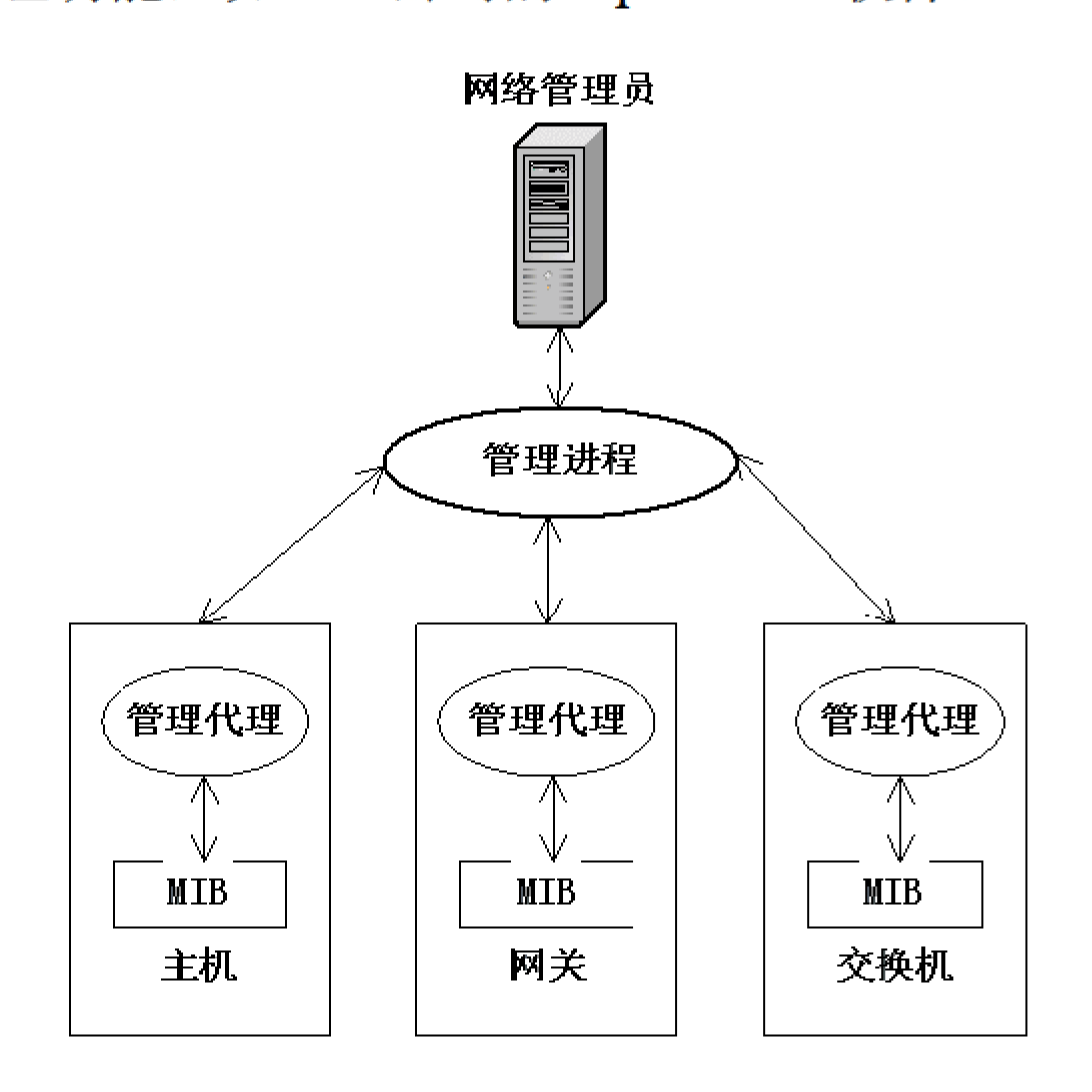


图 9.1　SNMP 网络管理模型的结构

2. 实际网络管理系统的组成

前面介绍的是 SNMP 网络管理模型的结构，而实际的网络管理系统往往有所区别。比如，实际的网络管理系统的组成如图 9.2 所示，由 4 个基本部分组成。

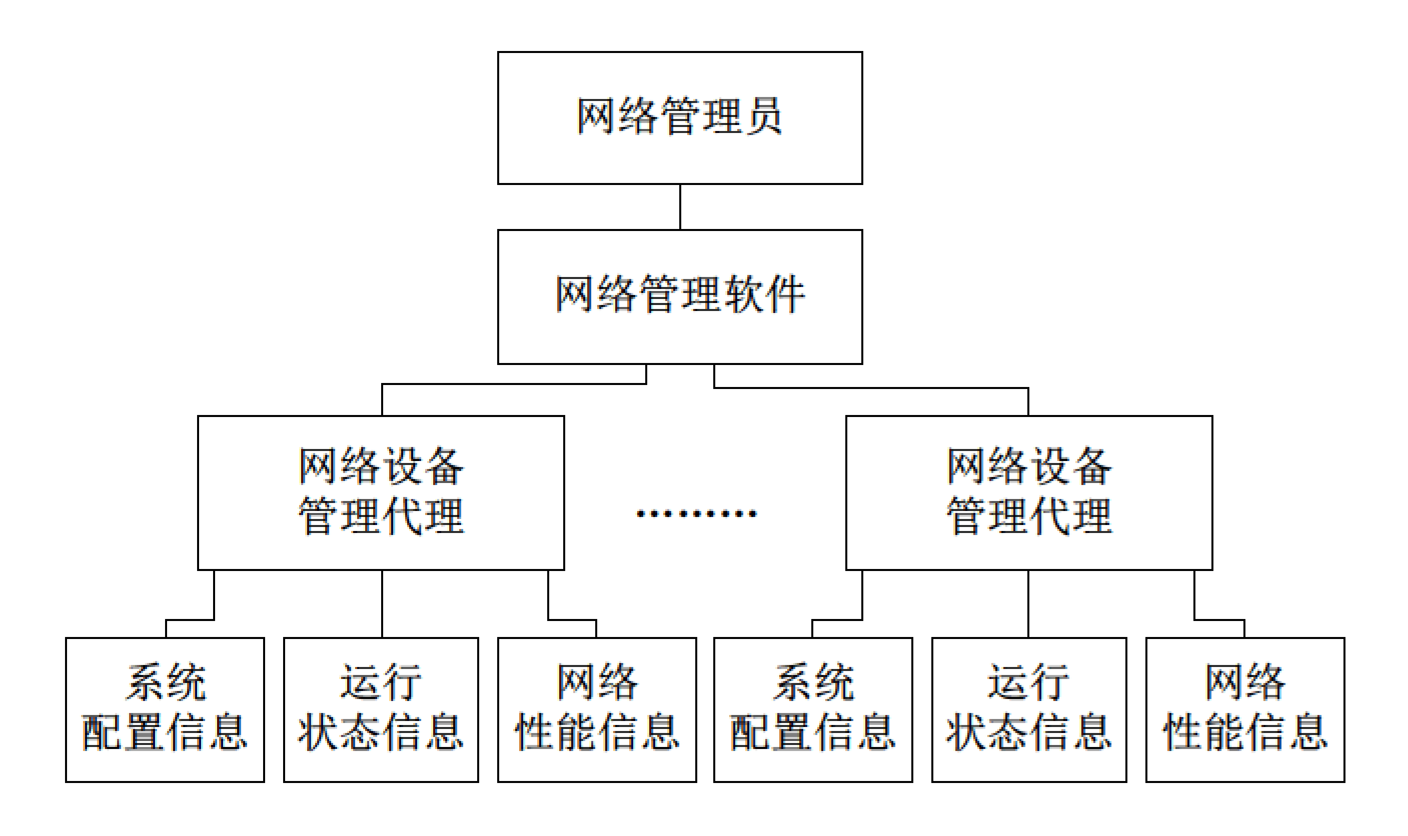


图 9.2　网络管理系统的组成结构

在大部分的实际网络管理系统中，只有前 3 个部分，因此这 3 个部分是基本的和必需的，而并非所有的网络都有“代理设备”，因此，第 4 个部分是可选的。下面将分别介绍这几个基本部分的功能和工作联系。

1)　网络管理软件

网络管理软件简称网管软件，它是协助网络管理员对整个网络或网络中的设备进行日常管理工作的软件。网络管理软件除了要求网络设备的“管理代理”定期采集用于管理的



各种信息外，还要定期查询管理代理采集到的与主机有关的信息，如系统配置信息、运行状态信息和网络性能信息等。网管软件正是利用这些信息来确定和判断整个网络、网络中的独立设备或者局部网络的运行状态是否正常。

在网络管理系统中，网络管理软件是连接其他几个因素的桥梁，因此占有着举足轻重的地位。它的功能的好坏将直接影响到整个网络管理系统的功能。

对于大型网络来说，网络规模较大且结构复杂，一旦网络出现故障，查找与维护都很困难。因此，网络管理软件是不可缺少的助手。而对于小型网络或个人用户来说，他们的技术水平较低，聘请专业技术人员的费用又太高，因此网络管理软件可以帮助解决一些棘手的问题。由此可见，网络管理软件已经成为各种网络中必不可少的组成部分。

市场上的网络管理软件名目繁多，因此选择网管软件已成为很多用户关心的问题。选择时可以从以下几个方面进行考虑： 与自身的管理规模和网络模式(如 C/S)相适应；具有智能化的监视能力；具有基于用户策略的控制能力；具有支持多协议、开放式操作系统和第三方管理软件的能力；具有良好的用户界面；具备简单的、无须编程的开发工具；具有良好的技术支持和服务；合适的性能价格比。

2) 网络设备的管理代理

网络设备的管理代理简称管理代理，它是驻留在网络设备中的一个软件模块。其中的网络设备可以是系统中的网络计算机、网络打印设备和交换机等。网络设备的管理代理软件能够获得每个网络设备的各种信息，如设备运行状况、系统配置、设备特性和性能等信息。因此，每个管理代理上的软件就像被管理设备的代理人，它可以完成网管软件所布置的信息采集任务。实际上，它充当了网络管理系统与被管理设备之间的信息中介。管理代理通过被控制设备中的 MIB 来实现管理网络设备的功能。

在实际应用中，由于 SNMP 协议确立了不同设备、软件和系统之间通信的基础框架。因此，人们通常选用支持 SNMP 协议的网络设备，如选择支持 SNMP 协议的服务器、路由器、交换机和集线器等。这样驻留在其中的管理代理软件就具有了共同语言。正因为有了这个标准语言，网络设备的管理代理软件才可以将网络管理员软件发出的命令按照统一的网络格式进行转化，再收集需要的信息，最后返回正确的响应信息，从而实现了网管软件在网络管理系统中的统一网络管理。

3) 管理信息库(MIB)

如前所述，MIB 定义了一种有关对象的数据库，它由网络管理系统所控制。整个 MIB 中存储了多个(可多达上千个)对象的各种信息数据。网管软件(在 SNMP 模型中又称管理进程)正是通过控制每个对象的 MIB 来实现对该网络设备的配置、控制和监视的。而网络管理员使用的网络管理系统可以通过网络管理的代理软件(管理代理)来控制每个 MIB 对象。

4) 代理设备

在网络管理系统中，代理设备是标准的网络协议软件和不支持标准协议的软件之间的一座桥梁。利用代理设备，无须升级整个网络管理系统即可实现旧版本网管软件到新版本的升级。例如，某网络正在使用的是支持旧版本 SNMP 协议的网管软件，当新版本 SNMP 协议开发出来后，如果直接升级则整个网络中所有的现存设备都会受到影响，使用代理设备则可以方便地解决此类问题。注意，正是由于代理设备的上述特殊功能，所以不是所有的网络管理系统中都有这种设备，也就是说，代理设备在网络管理系统中是可选的。



9.1.4　网络管理工具

由于网络管理已经有了一系列的标准，以及 OSI 定义的网络管理五大功能，使得具有配置管理、性能管理、故障管理、安全管理和计费管理五大功能的管理系统成为可能。同时，也正是得益于这样的网络管理系统，才能对网络进行充分、完备和有序的管理。但是由于涉及众多的网络管理协议和 5 个方面所要求的功能以及不同网络的实际情况，使得网络管理系统在技术上具有很强的挑战性。

网络管理系统是对以上几个基本要素的组合。大致可以将网络管理系统划分为 3 代。

第一代网管就是最常用的命令行方式，并结合一些简单的网络监测工具，它不仅要求使用者精通网络的原理及概念，还要求使用者了解不同厂商的不同网络设备的配置方法。这种方式的优点是具有很大的灵活性；缺点是风险系数增大，容易引发误操作，而且不具备图形化和直观性，比如网络探测工具 NetXray 可以运行在多种协议之下，包括 TCP/IP、SPX/IPX 等，工作在网络环境的底层，拦截所有正在网络上传输的数据并进行筛选处理，实时分析网络状态和设备布局，但第一代网管工具只能统计和分析网络的数据，并不能监控设备的状态，因此需要配合一系列 CLI 命令直接在设备上查看系统和端口信息。

第二代网管有着良好的图形化界面，用户无须过多了解设备的配置方法，就能图形化地对多台设备同时进行配置和监控，大大提高了工作效率，但仍然存在由于人为因素造成的设备功能使用不全面或不正确的问题，比如 CiscoView 是一个基于 GUI 的设备管理软件应用程序，可以图形的方式显示 Cisco 的物理视图。另外，它还提供配置和监视功能以及基本的故障排除功能。借助 CiscoView 可以更容易地理解设备提供的大量管理数据，网络管理员无须对远程站点上的每台设备进行物理检测就能够全面查看 Cisco 产品。

第三代网管相对来说比较智能，是真正将网络和管理进行有机结合的软件系统，具有“自动配置”和“自动调整”功能，对网管人员来说，只要把用户情况、设备情况以及用户与网络资源之间的分配关系输入网管系统，系统就能自动地建立图形化的人员与网络的配置关系，并自动鉴别用户身份，分配用户所需的资源(如电子邮件、Web、文档服务等)，同时，整个企业的网络安全得以保证；因此第三代网管系统是企业级的管理平台，由多个软件包构成，涉及 OSI 的 7 层协议集。目前第三代系统可选的范围比较广，如 CA Unicenter TNG、CiscoWorks2000、HP OpenView、IBM Tivoli、APRISMA Spectrum 等。这些网管软件通常包括一系列的子系统，有些子系统具有第二代系统的功能，如 CiscoWorks 中的 CiscoView。有些系统集成了其他系统的一些子系统以增强功能。

虽然网管系统发展到了第三代，但并不等于前两代系统已经淘汰，如何选择在于用户具体的网络管理需求，这 3 代系统分别适应不同的网络规模和网络应用，系统结构越是趋同，所需要的网管系统就越简单。而复杂的异构环境则需要完全成熟的企业管理软件。

国内网管软件近几年也取得一定的发展，但总体来说较大型的成熟的软件不多，国产软件的优势在于本地化，用户对界面的可操作性强，但大部分软件只相当于国外第三代网管系统中的某个子系统功能，网络的监控功能比较强，缺乏自动解决问题和管理用户资源的能力，而且软件更新和售后服务连贯性不强。总体来说，目前国内网管软件比较适用于中等规模企业或作为大型网管系统的辅助工具。

用户在选购网管软件时，必须结合具体的网络条件，网管软件用于辅助日常网络管理，



以提高管理效率，所以选择的软件应该体现有效管理原则。目前市场销售的网络管理软件可以按功能划分为网元管理(主机系统和网络设备)、网络层管理(网络协议的使用、LAN 和 WAN 技术的应用以及数据链路的选择)、应用层管理(应用软件)个层次，其中最基础的是网元管理，最上层的是应用层管理。

下面将介绍一种网络管理系统。以惠普(HP)公司的 OpenView 为代表，分析网络管理工具的特点。

HP 的 OpenView 有争议地成为第一个真正兼容的、跨平台的网络管理系统，因此也得到了广泛的市场应用。但是，虽然 OpenView 被认为是一个企业级的网络管理系统，但它跟大多数别的网络管理系统一样，不能提供 NetWare、SNA、DECnet、x.25，无线通信交换机以及其他非 SNMP 设备的管理功能。另外，HP 努力使 OpenView 由最初的提供给第三方应用厂商的开发系统，转变为一个跨平台的最终用户产品。它的最大特点是被第三方应用开发厂商所广泛接受。比如 IBM 就把 OpenView 增强功能并扩展成为自己的 NetView 产品系列，从而与 OpenView 展开竞争。特别在最近几年，OpenView 已经成为网络管理市场的领导者，与其他网络管理系统相比，OpenView 拥有更多的第三方应用开发厂商。在近期，OpenView 看上去更像一个工业标准的网络管理系统。

1. 网络监管特性

OpenView 不能处理因为某一网络对象故障而误导致的其他对象的故障。具体说来就是，它不具备理解所有网络对象在网络中相互关系的能力，因此一旦这些网络对象中的一个发生故障，导致其他正常的网络对象停止响应网络管理系统，它会把这些正常网络对象当作故障对象对待。同时，OpenView 也不能把服务的故障与设备的故障区分开来，比如是服务器上的进程出了问题还是该服务器出了问题，它不能区分。这些是 OpenView 的最大弱点。

另外，在 OpenView 中，性能的轮询与状态的轮询是截然分开的，这样导致一个网络对象响应性能轮询失败但不触发一个报警，仅仅只有当该对象不响应状态的轮询才进行故障报警。这将导致故障响应时间的延长，当然两种轮询的分开将带来灵活性上的好处，第三方的开发商可以对不同轮询的事件分别处理。

OpenView 还使用了商业化的关系数据库，这使得利用 OpenView 采集来的数据开发扩展应用变得相对容易。但第三方应用开发厂商需要自己找地方存放自己的数据，这又限制了这些数据的共享。

2. 管理特性

OpenView 的 MIB 变量浏览器相对而言是最完善的，而且正常情况下使用该 MIB 变量浏览器只会产生很少的流量开销。但 OpenView 仍然需要更多、更简洁的故障工具以应对各种各样的故障与问题。

3. 可用性

OpenView 的用户界面显得干净且相对灵活，但在功能引导上显得笨拙。同时 OpenView 还在简单、易用的 Motif 的图形用户界面上提供状态信息和网络拓扑结构图形，虽然这些信息和图形在大多数网络管理系统中都提供。但有个问题是 OpenView 的所有操作(至少现

在)都在 X-Windows 界面上进行，它还缺乏一些其他的手段，比如 WWW 界面和字符界面，同时它还缺乏开发基于其他界面应用的 API。

4. 总结

OpenView 是一个昂贵的，但相对够用的网络管理系统，它提供了基本层次上的功能需求。它的最大优势在于它被第三方开发厂商所广泛接受。但得到了 NetView 许可证的 IBM 已经加强并扩展了 OpenView 的功能，以此形成了 IBM 自己的 NetView/6000 产品系列，该产品可以在很大程度上视为 OpenView 的一种替代选择。

9.2　计算机网络维护方法

随着计算机的广泛应用和网络的流行，目前单位内广大职工的很多日常工作(包括生产 MIS、电力营销、视频监控、集群录音等各种系统)已经与网络密不可分，计算机网络系统就是利用通信设备和线路将地理位置不同的、功能独立的多个计算机系统互联起来，以功能完善的网络软件(网络通信协议、信息交换方式及网络操作系统等)实现网络中资源共享和信息传递的系统。它的主要功能表现在两个方面：一是实现资源共享，包括硬件资源和软件资源的共享；二是在用户之间交换信息。因此，如何有效地做好本单位计算机网络的日常维护工作，确保其安全、稳定地运行，这是网络运行维护人员的一项非常重要的工作。

9.2.1　故障定位的基本思路

在排除比较复杂网络的故障时，常常要从多种角度来测试和分析故障的现象，准确确定故障点，在实际应用中通常采用的分析模型和方法如下。

(1) 7 层的网络结构分析模型方法。从网络的 7 层结构的定义和功能上逐一进行分析和排查，这是传统的且最基础的分析和测试方法。这里有自下而上和自上而下两种思路。自下而上是从物理层的链路开始检测直到应用，自上而下是从应用协议中捕捉数据包，分析数据包统计和流量统计信息，以获得有价值的资料。

(2) 网络连接结构的分析方法。从网络的连接构成来看，大致可以分成客户端、网络链路、服务器端 3 个模块。

客户端具备网络的 7 层结构，也会出现从硬件到软件、从驱动到应用程序、从设置错误到病毒等的故障问题。所以在分析和测试客户端的过程中要有大量的背景知识，有时 PC 发烧友的经验也会有所帮助，也可以在实际测试过程中询问客户端的用户，分析他们反映的问题是个性的还是共性的，这将有助于自己对客户端的进一步检测作出决定。

来自网络链路的问题通常需要网管、现场测试仪，甚至需要用协议分析仪来帮助确定问题的性质和原因。对于这方面的问题分析需要有坚实的网络知识和实践经验，有时实践经验会决定排除故障的时间。

在分析服务器端的情况时更需要有网络应用方面的丰富知识，要了解服务器的硬件性能及配置情况、系统性能及配置情况、网络应用及对服务器的影响情况。

工具型分析方法。有强大的各种测试工具和软件，它们的自动分析能快速地给出网络的各种参数甚至是故障的分析结果，这对解决常见网络故障非常有效。



综合及经验型分析方法。靠时间、错误和成功经验的积累，在大多数的网络维护工作人员的工作中是采用这个方法的，再依靠网管和测试工具迅速定位网络的故障。

9.2.2 计算机常见故障分类

1. 某台计算机上不了网

对于某台计算机上不了网的故障，首先要分别确定此计算机的网卡安装是否正确，是否存在硬件故障，网络配置是否正确，如在实际工作中一般采用 Ping 192.168.131.1 来判断网卡硬件安装和 TCP/IP 协议的正确性。如果能 Ping 通，即说明这部分没有问题。如果出现超时情况，则要检查计算机的网卡是否与机器上的其他设备存在中断冲突的问题。通过查看系统属性中的设备管理器，查看是否在网络适配器的设备前面有黄色惊叹号或红色叉号，如有则说明硬件的驱动程序没有安装成功，可删除后重新安装。另外，要确保 TCP/IP 协议安装的正确性，并且要绑定在所安装的网卡上。如果重新安装后还是 Ping 不通回送地址，最好换上一块正常的网卡试一试。由于在局域网中划分了 VLAN，所以连在不同 VLAN 中的计算机都有各自不同的 IP 地址、子网掩码和网关。要在机器的网络属性中设定的 IP 地址等数据与连接的 VLAN 相匹配；否则将出现网络不通的情况。当确保计算机的硬件设备和网络配置正确后，接着就要查看计算机与交换机之间的双绞线以及交换机的 RJ-45 端口或交换机的配置是否有问题。此时要 Ping 上网计算机所在 VLAN 的网关，不通的话就要分段检查上面所说的各项，最简单的方法是检查双绞线，用线缆测试仪检测双绞线是否断开，若双绞线没有问题，就要查看交换机的端口是否坏了。交换机每一个端口都有状态指示灯，检测到此，如果端口指示灯不亮，就只能是端口损坏了，可以把跳线接到正常使用的端口上排除其他原因，确定是端口的问题。另外，还有交换机的配置问题，只有极少的几个人对交换机的配置有修改权限，所以询问一下其他网管人员就可以排除了，如果不放心可以对照查看。交换机的参数配置表也是网络管理员必备的资料之一，并且随着网络用户的变化要不断地修改。

2. 多台计算机上不了网

对于同时有多台计算机上不了网的故障，首先要找到这些计算机的共性，如是不是属于同一 VLAN 或接在同一交换机上的，若这些计算机属于同一 VLAN，且属于计算机分别连接于不同的楼层交换机，那么检查一下路由器上是否有 AC1 限制，在路由器上对该 VLAN 的配置是否正确，路由协议是否配置正确。若这些计算机属于同一交换机，则应到机房检查该交换机是否有电源松落情况，或该交换机 CPU 负载率是否很高，与上一级网络设备的链路是否正常，通常某交换机连接的所有计算机都不能正常与网内其他计算机通信，这是典型的交换机死机现象，可以通过重新启动交换机的方法解决。如果重新启动后故障依旧，则检查一下那台交换机连接的所有计算机，看逐个断开连接的每台计算机的情况，慢慢定位到某个故障计算机，会发现多半是某台计算机上的网卡故障导致的，故障通常是交换机的某个端口变得非常缓慢，最后导致整台交换机或整个堆叠慢下来，通过控制台检查交换机的状态，发现交换机的缓冲池增长得非常快，达到了 90%或更多，原因及解决方法是首先应该使用其他计算机更换这个端口上原来的连接，看是否由这个端口连接的那台计算机的网络故障导致的，也可以重新设置出错的端口并重新启动交换机，有时可能是这个端口



损坏了。

3. 链路问题

当链路是光缆时，在开通新的网络时，应记录光缆的收发光功率、光缆长度和芯数，一旦出现问题应重新用光功率计、OTDR 等再次测试，并与原来数据进行比较后及时修复。若链路是网线，如办公室内的，则可通过网络一点通等网络测试仪确定办公室至交换机之间的哪段网线出了问题。

4. 机柜接地问题

机柜接地不能忽略，如曾经发生过市局为一台 C2MFT G703 接口模块、更换 Cisco 6509，市局端更换 Cisco 3550 的 2M 的连接端口，更换 SDH 的 2M 链路均无效的事件，最终在县局 Cisco 6509 采用 WIC IT 模块加外接协议转换器，网络互联恢复正常。准备再次采用 VWIC 2MFT G703 接口模块，在拆外接协议转换器时被触了一下电，再仔细查找机柜的接地线，没有找到，给机柜接上地线后，再采用原来设备，一切恢复正常。分析结果，外接协议转换器输出信号的电压较高，所以抗干扰能力强，尽管没有接地，但因无接地而产生的干扰不对它产生影响，所以网络互联正常。而 Cisco 的 VWIC 2MFT G703 接口模块输出信号的电压较低，和无接地产生的干扰差不多，从而因输出信号遭到破坏而导致 SDH 2M 误码告警；路由器的端口不断 up 和 down。由此可见，机柜接地看似小问题，如果没做好也会带来很大的麻烦。

9.2.3　故障定位及排除的常用方法

1. 告警性能分析法

通过网管获取告警和性能信息进行故障定位。例如，某一供电局使用了 BTTA 网管，可以对全局的网络设备进行管理，平时多观察各设备 CPU 负载率和各线路的流量，当有人反映不能连接至网络或网速很慢时，可通过网管观察计算机与交换机的连接情况，是否有时断时通的现象，交换机 CPU 负载率是否很高，线路流量是否很大，通过观察设备端口状态，分析和观察交换机哪个端口所接的计算机发包量不太正常。

2. 替换法

替换法就是使用一个工作正常的物体去替换一个工作不正常的物体，从而达到定位故障、排除故障的目的，这里的物件可以是一段线缆、一个设备和一块模块。

3. 配置数据分析法

查询、分析当前设备的配置数据，通过分析以上的配置数据是否正常来定位故障，若配置的数据有错误，需进行重新配置。

9.2.4　计算机网络的维护

1. 维护内容

计算机网络的维护内容包括设备、链路、电源和配线架等附属设备的维护。具体要求



如下。

(1) 保证设备工作条件，包括供电条件和环境条件等。

(2) 对系统故障进行判断和处理，根据故障现象和告警指示，利用网管及各种测试工具进行故障定位，找出故障原因，在最短时间内排除故障。

(3) 通常采用集中维护方式，将维护人员和必要的维护仪表集中在一个主要站。

(4) 经常检查交换机与路由器中的端口状态，尤其需要关注端口差错统计信息，对于出错包特别多的端口，应该检查其是交换机或路由器本身的、链路的原因，还是接入设备的原因。交换机或路由器主要查询 CPU 的利用率和 MEM 的利用率，接入设备若是计算机，则主要看网卡的设置是否正确、网卡的驱动程序是否和网卡相匹配，查出原因后进行整改，检查完后对端口统计信息清零。

(5) 链路若是光缆，则主要检查现有衰耗和投运时的衰耗差，链路是网线则用专用仪器进行现场测试，光纤不允许小角度弯折，更不能出现直角。

(6) 网管监控系统和本地维护终端用的计算机是专用设备，禁止挪用，以免病毒侵害。

2. 对维护人员的要求

(1) 对运行中的网络设备在进行变更设置的操作时，必须有两人同时在场方可进行，一人操作，一人监护，并做好如何在操作失败而导致网络设备异常的情况下的处理预案，履行必要手续。

(2) 处理光接口信号时，不得将光发送器的尾纤端面或上面活动连接器的端面对着眼睛，并注意尾纤端面和连接器的清洁。

(3) 熟练掌握所维护设备的基本操作。

(4) 做好设备的日常巡视工作。

(5) 对外来人员(参观者或领导)应讲明道理，关照他请勿动手。

计算机网络建设越来越庞大，且组网方式繁多而复杂，自然就加大了维护人员的工作量和故障定位、处理的难度，这就要求维护人员必须不断提高自身的业务水平和处理故障的能力，同时要针对实际情况，把以上的定位原则和处理方法做到灵活应用。

9.3 Windows 自带的网络工具

随着网络技术与应用的不断发展，计算机网络在人们的日常生活中已经变得越来越普及。特别是 20 世纪 90 年代以来，随着 Internet 在世界范围内的普及，计算机网络已经逐渐成为人们获取信息、发布信息的重要途径。与此同时，基于计算机网络的应用也越来越多，许多人们生活中的重要环节都可以利用网络方便、快捷地实现。这些网络的发展使得大到国家经济命脉小到个人日常生活严重依赖于计算机网络，因此网络运行的稳定性、可靠性就显得至关重要，于是网络维护应运而生。本节主要讨论网络维护的相关知识。

网络维护是计算机网络发展的必然产物，它随着计算机网络的进步而发展。早期的计算机网络主要是局域网，在一定范围内连接数百台计算机，因此最早的网络维护是局域网维护。由于局域网维护主要保证在局域网内的所有计算机能够顺利传递和共享文件，因此早期的局域网维护与网络操作系统密不可分。而 Internet 的出现打破了网络的地域限制，跨

地域的广域网络得到飞速发展，这时的网络维护不再局限于保证文件的传输，而是保障连接网络的网络对象(路由器、交换机、线路等)的正常运转，同时监测网络的运行性能，优化网络的拓扑结构。因此网络维护越来越复杂，功能也越来越完备，网络维护已发展成为计算机网络中的一个重要分支。

9.3.1　Ping 命令

Ping 用于确定本地主机是否能与另一台主机交换(发送与接收)数据包。根据返回的信息，可以推断 TCP/IP 参数设置是否正确，以及运行是否正常。需要注意的是，成功地与另一台主机进行一次或两次数据包交换并不表示 TCP/IP 配置是正确的，必须执行大量的本地主机与远程主机的数据包交换，才能确定 TCP/IP 的正确性。

Ping 命令是 Windows 中集成的一个专用于 TCP/IP 协议的探测工具。应用 TCP/IP 协议的局域网或广域网，当客户端与客户端之间无法正常进行访问或者网络工作出现各种不稳定的情况时，建议要先试试用 Ping 命令来确认并排除问题。

1. Ping 命令的语法格式

Ping 命令的语法格式：

Ping　目的地址　[-t] [-a] [-n count] [-l size] [-w timeout]

其中：目的地址是指被测试计算机的 IP 地址或域名。

主要参数功能说明：

- -t —— 用当前主机不断向目的主机发送数据包，直到用户按 Ctrl+C 快捷键终止。
- -a——解析主机地址。
- -n count ——发出的测试包的个数，默认值为 4。
- -l size —— 指定发送数据包的大小，默认值为 32。
- -w timeout —— 指定超时时间的间隔(单位为 ms，默认值为 1000)。

通常，使用较多的参数是-t、-n、-w。Ping 的其他参数，可通过在 DOS 的提示符下输入 Ping 或 Ping-？命令来查看相关帮助信息。

例如：DOS 提示符下或在 Windows 开始菜单的运行中输入：

```
Ping IP -t
```

连续对 IP 地址执行 Ping 命令，直到被用户以按 Ctrl+C 快捷键中断。

```
Ping IP -l 3000
```

指定 Ping 命令中的数据包长度为 3000B，而不是默认的 32B。

```
Ping IP -n
```

执行 n 次 Ping 命令。

Ping 命令用来检测一帧数据从本地传送到目的主机所需的时间。它通过发送一些小的数据包并接收应答信息来确定两台计算机之间的网络连接情况。

如果执行 Ping 不成功，则可以预测故障出在以下几个方面：

①　网线没有连通。



② 网络适配器配置不正确。

③ IP 地址不可用。

如果 Ping 程序成功返回而网络仍无法使用，那么问题很可能出在网络系统的软件配置方面。Ping 成功只能保证本地与目的主机存在一条连通的物理途径。

【例 9.1】 检查网络服务器和任意一台客户端上 TCP/IP 协议的工作情况。

在网络中其他任何一台计算机上 Ping 该计算机的 IP 地址即可。

在 DOS 命令提示符下输入：

```
Ping 192.192.225.225
```

如果 TCP/IP 协议工作正常，会以 DOS 屏幕方式显示以下所示的信息：

```
Pinging 192.192.225.225 with 32 bytes of data:
Reply from 192.192.225.225:bytes=32 time=1ms TTL=128
Reply from 192.192.225.225:bytes=32 time<1ms TTL=128
Reply from 192.192.225.225:bytes=32 time<1ms TTL=128
Reply from 192.192.225.225:bytes=32 time<1ms TTL=128

Ping statistice for 192.192.225.225:
Packets:Sent=4,Received =4,Lost =0(0% loss)
Approximate round trip times in milli-seconds:
Minimum=0ms,Maximum=1ms,Average=0ms
```

以上返回了 4 个测试数据包，其中 bytes=32 表示测试中发送的数据包大小是 32B，time<1ms 表示与对方主机往返一次所用的时间小于 1ms，TTL=128 表示当前测试使用的 TTL(Time To Live)值为 128(系统默认值)。

按照默认设置，Windows 上运行的 Ping 命令发送 4 个 ICMP(网间控制报文协议)回送请求，每个 32 B 数据，如果一切正常，应能得到 4 个回送应答。

Ping 能够以 ms 为单位显示发送回送请求到返回回送应答之间的时间。如果应答时间短，表示数据包不必通过太多的路由器或网络连接速度比较快。Ping 还能显示 TTL(Time To Live，存在时间)值，可以通过 TTL 值推算数据包已经通过了多少个路由器，源地点 TTL 起始值(就是比返回 TTL 略大的一个 2 的乘方数)返回时 TTL 值。例如，返回 TTL 值为 119，那么可以推算数据包离开源地址的 TTL 起始值为 128，而源地点到目标地点要通过 9 个路由器网段(128～119)；如果返回 TTL 值为 246，TTL 起始值就是 256，源地点到目标地点要通过 9 个路由器网段。

如果网络有问题，则返回以下响应失败信息：

```
Pinging 192.192.225.225 with 32 bytes of data
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistice for 192.192.225.225:
Packets: Sent=4,Received =0,Lost=4(100% loss),
Approximate round trip times in milli-seconds
Minimum=0ms,Maximum=0ms,Average=0ms
```

出现此种情况时，就要仔细分析一下网络故障出现的原因和可能有问题的网上节点了，建议从以下几个方面来着手排查。

① 检查计算机是否已安装了 TCP/IP 协议。

② 检查计算机的网卡安装是否正确且是否已经连通。

③ 检查计算机的 TCP/IP 协议是否与网卡有效地绑定(具体方法是通过选择【开始】|【设置】|【控制面板|网络】来查看)。

④ 检查 Windows 服务器的网络服务功能是否已启动(可通过选择【开始】|【设置】|【控制面板】|【服务】，在出现的对话框中找到“Server”一项，看“状态”下所显示的是否为“已启动”)。

如果通过以上 4 个步骤的检查还没有发现问题的症结，应重新安装并设置 TCP/IP 协议；如果是 TCP/IP 协议的问题，可以彻底解决问题。

按照上述方法，还可以用 Ping 命令来检查任意一台客户端计算机上 TCP/IP 的工作情况。例如，要检查网络任一客户端“机房 01”上的 TCP/IP 协议的配置和工作情况，可直接在该台机器上 Ping 本机的 IP 地址，若返回成功的信息，说明 IP 地址配置无误，若失败则应检查 IP 地址的配置。

可通过以下步骤进行：

首先检查整个网络，重点检查该 IP 地址是否正在被其他用户使用，再检查该工作站是否已正确连入网络(很多情况下用户没有登录网络也会出现此种情况)。最后检查网卡的 I/0 地址、IRQ 值和 DMA 值是否与其他设备发生冲突。其中最后一项的检查非常重要，也常被许多用户所忽视，即使是 Ping 成功后也要进行此项的检查。因为当 Ping 本机的 IP 地址成功后，仅表明本机的 IP 地址配置没有问题，但并不能说明网卡的配置完全正确。这时虽然在本机的“网上邻居”中能够看到本机的计算机名，可无法与其他的用户连通，问题往往就出在网卡上。

如果在 Windows【开始】|【运行】命令的对话框中输入 Ping 命令，命令能够执行，但上述显示结果后关闭显示窗口。在 Windows 的【开始】|【运行】命令的对话框中执行 Ping 命令应加-t 参数，表示连续对 IP 地址执行 Ping 命令，直到被用户按 Ctrl+C 快捷键中断。

【例 9.2】 检查本机与某网址的正常通信情况。

在 DOS 命令提示符下输入:

```
Ping  www.263.net
```

DOS 屏幕显示以下所示的信息:

```
Pinging www.263.net[211.100.31.131] with 32  bytes of data:
Reply from 211.100.31.131: bytes=32 time=50ms TTL=243
Reply from 211.100.31.131: bytes=32 time=60ms TTL=243
Request timed out.
Reply from 211.100.31.131: bytes=32 time=50ms TTL=243
Ping statistics for 211.100.31.131:
Packets: Sent=4, Received=3, Lost: 1(25%loss),
Approximate round trip times in mili-seconds:
Minimum=50ms, Maximum=60ms, Average=53ms
```



从上面的返回结果可以知道，向 www.263.net(其 IP 为 211.100.31.131)发送的 4 个大小为 32B 的测试数据包中，有 3 个得到了服务器的正常响应(Reply from…)，另一个响应超时(Request timed out)。平均每个数据包自发送到收到服务器响应的时间间隔为 56ms(最小为 50ms，最大为 60ms)。

这一结果显示，本机到 www.263.net 的网速较快(平均响应时间短)，但是网络可能不大稳定(丢失了一个数据包)。

【例 9.3】 检查本机与某网址的通信异常情况。

在 DOS 命令提示符下输入:

```
Ping  202.11.89.118
Pinging 202.112.89.118 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 202.112.89.118:
Packets: Sent=4, Received=0, Lost=4(100%loss),
Approximate round trip times in milli-seconds:
Minimum=0ms, Maximum=0ms, Average=0ms
```

例 9.3 中 4 个测试数据包均超时，说明本机很可能无法与 202.112.89.118 通信。

但是也存在例外情况，即 Ping 不连通但实际网络是连通的。这是因为 Ping 命令用来检测最基本的网络连接情况，它所使用的数据包为 TCP/IP 协议族最基本的 ICMP 包。但是某些操作系统(尤其是 Windows)存在缺陷，面对对方发送过来的大的 ICMP 包，或者数量巨大的碎小的 ICMP 包，无法正常处理，可能导致网络堵塞、瘫痪，甚至整个系统崩溃、死机。目前的网络防火墙对发来的 ICMP 包不做任何处理，应直接抛弃。在 Ping 装有这样的防火墙的主机时，将被告知“Request time out”，其实这并不是网络不通。

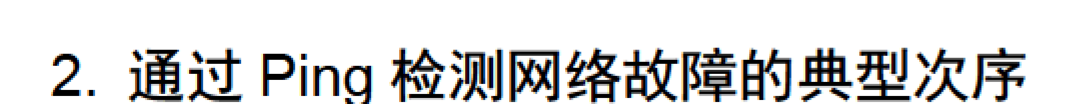
【例 9.4】 某一网站的网页无法访问的情况。

在 DOS 命令提示符下输入:

```
Ping noabcd.com
Unknown host noabcd .com.
```

这一结果显示域名 noabcd .com 不存在。

Ping 命令不仅在局域网中广泛使用，在 Internet 中也经常使用它来探测网络的远程连接情况。当遇到以下两种情况时，需要利用 Ping 工具对网络的连通性进行测试。比如当某一网站的网页无法访问时，可使用 Ping 命令进行检测。如果返回类似于 Pinging ns. rising.com.cn with 32 bytes of data:…的信息，说明对方的主机已打开，相反则表明在网络连接的某个环节出现故障，或对方的主机未打开。另外，在发送 E-mail 之前也可以先测试一下网络的连通性。许多用户在发送 E-mail 后经常收到诸如 Returned mail:User unknown 的信息，这说明邮件未发送到目的地。要想避免此类事件再次发生，建议发送 E-mail 之前先养成 Ping 对方邮件服务器地址的习惯。例如，当给 fbk@***.net 发送邮件时，可先输入 Ping ***.net 进行测试，如果返回类似于 Bad IP address cniti.com 或 Request times out 的信息，说明对方的主机未打开或网络未连通。这时即使将邮件发出去，对方也无法收到。



2. 通过 Ping 检测网络故障的典型次序

正常情况下，当使用 Ping 命令来查找问题所在或检验网络运行情况时，需要使用许多 Ping 命令，如果运行正确，就可以相信基本的连通性和配置参数没有问题；如果某些 Ping 命令出现运行故障，它也可以指明到何处去查找问题。

下面给出一个典型的检测次序及对应的可能故障。

1) Ping 127.0.0.1

验证本机 TCP/IP 协议是否安装好。

如出现以下显示，则表示本机 TCP/IP 协议安装完好：

```
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Ping statistics for 127.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

否则如出现以下显示，则表示本机 TCP/IP 协议安装不完整，请重新添加 TCP/IP 协议：

```
Pinging 127.0.0.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out
Ping statistics for 127.0.0.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2) Ping 本机 IP

验证本机 IP 地址是否配置完成或者网卡物理属性是否完好。

如出现以下显示，则表示本机 IP 地址已配置好且网卡物理属性完好：

```
Pinging 202.201.14.55 with 32 bytes of data:
Reply from 202.201.14.55: bytes=32 time<10ms TTL=128
Reply from 202.201.14.55: bytes=32 time<10ms TTL=128
Reply from 202.201.14.55: bytes=32 time<10ms TTL=128
Reply from 202.201.14.55: bytes=32 time<10ms TTL=128
Ping statistics for 202.201.14.55:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

否则如出现“Request timed out.”，则表示本机 IP 地址未配置好或网卡物理属性不好，请配置好 IP 地址，如果还有问题请更换网卡或重新安装网卡驱动程序。



3) Ping 局域网内其他 IP

命令经过网卡及网络电缆到达其他计算机，再返回。收到回送应答表明本地网络中的网卡和载体运行正确。但如果收到 0 个回送应答，那么表示子网掩码(进行子网分割时，将 IP 地址的网络部分与主机部分分开的代码)不正确，或网卡配置错误或电缆系统有问题。

4) Ping 网关 IP

验证本机到网关的物理线路是否连通。

如显示“Reply from.....”，则表示本机到网关物理线路连通性完好；如显示“Request timed out.”，则表示本机到网关物理线路连通性有故障，请联系网管解决。

5) Ping 远程 IP

如果收到 4 个应答，表示成功地使用了默认网关。对于拨号上网用户则表示能够成功地访问 Internet(但不排除 ISP 的 DNS 会有问题)。

6) Ping localhost

localhost 是系统的网络保留名，也是 127.0.0.1 的别名，每台计算机都应该能够将该名字转换成该地址。如果没有做到，则表示主机文件中存在问题。

7) Ping www.xxx.com(如 www.yesky.com 天极网)

对域名执行 Ping www.xxx.com 地址，通常是通过 DNS 服务器，如果这里出现故障，则表示 DNS 服务器的 IP 地址配置不正确或 DNS 服务器有故障(对于拨号上网的用户，某些 ISP 已经不需要设置 DNS 服务器了)。也可以利用该命令实现域名对 IP 地址的转换功能。

如果上面所列出的所有 Ping 命令都能正常运行，那么本地计算机进行本地和远程通信的功能基本上就可以放心了。但是，这些命令的成功并不表示所有的网络配置都没有问题，如某些子网掩码错误就可能无法用这些方法检测到。

9.3.2 Ipconfig/Winipcfg 命令

Winipcfg 和 Ipconfig 都是用来显示主机内 IP 协议的配置信息。只是 Winipcfg 适用于 Windows 9X/Windows Me，而 Ipconfig 适用于 Windows NT/2000/XP。

利用 Ipconfig 和 Winipcfg 命令可以查看和修改网络中的 TCP/IP 协议的有关配置，如 IP 地址、网关、子网掩码等，还可以查看与主机相关的信息，如主机名、DNS 服务器、节点类型等。其中网络适配器的物理地址在检测网络错误时非常有用。这两个工具功能基本相同，只是 Ipconfig 是以 DOS 的字符形式显示，而 Winipcfg 则用图形界面显示。

1. Ipconfig 命令

语法格式:

```
Ipconfig[/all][/batch file][/renew all][/release all][/renew n][/release n]
```

主要参数功能说明如下：

- all，显示与 TCP/IP 协议相关的所有细节信息，其中包括测试的主机名、IP 地址、子网掩码、节点类型、是否启用 IP 路由、网卡的物理地址及默认网关等。
  当使用 all 选项时，Ipconfig 能为 DNS 和 WINS 服务器显示必需的附加信息(如 IP 地址等)，并且显示本地网卡的物理地址(MAC)。如果 IP 地址是从 DHCP 服务器

租用的，Ipconfig 将显示 DHCP 服务器的 IP 地址和租用地址预计失效的日期。

- batch file，将测试的结果存入指定的 file 文件，以便逐项查看，如果省略 file 文件名，则系统会把该测试的结果保存在系统的 Winipcfg.out 文件中。
- renew all，更新全部适配器的通信配置情况，所有测试重新开始。
- release all，释放全部适配器的通信配置情况。
  发布当前的 DHCP 配置。该选项禁用本地系统上的 TCP/IP，并只在 DHCP 客户端上可用。可输入使用不带参数的 Ipconfig 命令显示的适配器名称。
- renew n，更新第 n 号适配器的通信配置情况，所有测试重新开始。
- release n，释放第 n 号适配器的通信配置情况。

如果没有参数，那么 Ipconfig 实用程序将向用户提供所有当前的 TCP/IP 配置值，包括 IP 地址和子网掩码。

【例 9.5】 更新 0 号适配器的 IP。

在 DOS 命令提示符下输入：

```
Ipconfig  /renew 0
```

【例 9.6】 显示本地 IP 配置的详细信息。

在 DOS 命令提示符下输入：

```
Ipconfig / all
```

显示结果如下：

```
Windows 2000 IP Configuration
Host Name............: WhatEver
Primary DNS Suffix.........:
Node Type.........: Hybrid
IP Routing Enabled.........: No
WINS Proxy Enabled.........: No
Ethernet adapter 本地连接:
Connection -specific DNS  Suffix . :
Description.........:  Realtek RTL8139/810X Family PCI   Fast Ethernet NIC
Physical  Address...........: 00-E0-4C-3A-28-E9
DHCP  Enabled...........: No
IP  Address...........: 162.105.81.179
Subnet  Mask...........: 255.255.255.0
Default  Gateway...........: 162.105.81.1
DNS  Servers...........: 202.112.1.12
                          202.112.1.13
```

2. Winipcfg 命令

Winipcfg 工具的功能与 Ipconfig 基本相同，只是 Winipcfg 是以图形界面的方式显示，在操作上更加方便。当用户需要查看任何一台机器上 TCP/IP 协议的配置情况时，只需在 Windows 9X/Windows Me 上选择【开始】|【运行】命令，在打开的对话框中输入命令 Winipcfg，将出现如图 9.3 所示 IP 配置对话框。

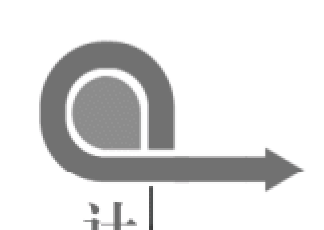




图 9.3　IP 配置对话框

图 9.3 中显示了网卡类型、网卡的物理地址、主机的 IP 地址、子网掩码、路由器的地址，如果用户想更详细地了解该主机的其他 IP 协议配置信息，如 DNS 服务器、DHCP 服务器等方面的信息，可以直接单击该界面中的详细信息按钮，在随后出现的对话框中查看和改变 TCP/IP 的有关配置参数。当一台机器上安装有多个网卡时，还可以查找到每个网卡的物理地址和有关协议的绑定情况等。

3. Ipconfig/Winipcfg 的应用

(1)　查找目标主机的 IP 地址及其他有关 TCP/IP 协议的信息。

选择【开始】|【运行】命令，打开【运行】对话框，输入 Winipcfg 命令，就会出现一个 IP 配置对话框，会显示有关目前网络 IP 的一些详细设置数据。

也可以在 MS-DOS 模式下，输入 Ipconfig 命令，在 DOS 窗口下显示详细的 IP 信息。

(2)　Ipconfig/Winipcfg 是一款网络侦察利器，尤其当用户的网络中设置的是 DHCP(动态 IP 地址配置协议)时，利用 Ipconfig/Winipcfg 可以很方便地了解到 IP 地址的实际配置情况。因为它有一个/all 参数，所以它可侦查到本机上所有网络适配的 IP 地址分配情况，比 Ping 命令更为详细。如果在计算机 bb_data 客户端上运行 Ipconfig/all/batch data.txt 后，打开 data.txt 文件，将能非常详细地显示所有与 TCP/IP 协议有关的配置情况。

与 Ping 相比，它的不足之处是只能在本机上测试，不能运用网络功能来测试。

9.3.3　Netstat 命令

Netstat 命令也是运行于 DOS 提示符下的工具，利用该工具可以显示有关统计信息和当前 TCP/IP 的网络连接情况，用户或网络管理人员可以得到非常详尽的统计结果。如系统网络连接的信息(使用的端口和在使用的协议等)，收到和发出的数据，被连接的远程系统的端口等。

1. Netstat 命令的语法格式

Netstat 格式：

```
Netstat [-a] [-p] [-n] [-r]  [-s]  [interval]
```

主要参数功能说明如下。

- -a，显示所有有效连接的信息列表，包括已建立的连接(ESTABLISHED)，也包括监听连接请求(LISTENING)的连接。通常用于获得本地系统开放的端口，还可以

检查是否被安装木马，如果机器上运行 Netstat 命令发现诸如 port 12345(TCP) netbus、port 31337(UDP) back orifice 之类的信息，则机器上就很有可能感染了木马病毒。

- -p，用来显示特定的协议配置信息，它的格式为 Netstat -p xxx，xxx 可以是 UDP、IP、ICMP 或 TCP，如要显示机器上的 TCP 协议配置情况可以用 Netstat -p tcp。
- -n，用数字显示地址和端口，通常用于检查自己的 IP，用数字的形式来显示主机名。
- -r，显示关于路由表的信息，除了显示有效路由外，还显示当前有效的连接。
- -s，显示默认情况下每个协议的配置统计，包括 TCP、IP、UDP、ICMP 等协议。能够按照各个协议分别显示其统计数据。如果应用程序(如 Web 浏览器)运行速度比较慢，或者不能显示 Web 页之类的数据，那么就可以用本选项来查看一下所显示的信息。
- interval，每隔 interval 秒重复显示所选协议的配置情况，直到按 Ctrl+C 快捷键中断。

在命令提示符下输入 Netstat/？可获得 Netstat 的使用帮助。命令中的一些参数是区分大、小写的。

2. Netstat 的应用

从以上各参数的功能可以看出 Netstat 工具有以下几个方面的应用。

(1) 显示本地或与之相连的远程机器的连接状态，包括 TCP、IP、UDP、ICMP 协议的使用情况，了解本地机开放的端口情况。

(2) 检查网络接口是否安装正确，如果在用 Netstat 这个命令后仍不能显示某些网络接口的信息，则说明这个网络接口没有正确连接，需要重新查找原因。

(3) 通过使用-r 参数查询与本机相连的路由器地址分配情况。

(4) 检查常见的木马程序，任何黑客程序都需要通过打开一个端口来达到与服务器进行通信的目的，不过首先要使计算机接入 Internet 才行，不然这些端口是不可能打开的，而且这些黑客程序也不会达到入侵的目的。

9.3.4 Tracert 命令

Tracert 主要用来显示数据包到达远程计算机所经过的路径。该命令能把送出的到某一远程计算机的请求包，所经过的全部路由都显示出来，如该路由的 IP 是多少、通过该 IP 的时延是多少等。

主要功能：判定数据包到达远程计算机所经过的路径、显示数据包经过的中继节点清单和到达时间。

1. Tracert 命令的语法格式

Tracert 命令格式：

```
Tracert [-d] [-h maximum_hops] [-j host_list] [-w timeout]
```

主要参数功能及说明如下：



- -d，不解析远程计算机的名字。
- -h maximum_hops，指定搜索到目标地址的最大跳跃数。
- -j host_list，按照计算机列表中的地址释放源路由。
- -w timeout，指定超时时间间隔，程序默认的时间单位是毫秒。

2. Tracert 的应用

要了解本地计算机与远程计算机之间详细的传输路径信息，可以使用 Tracert 命令。

在 DOS 命令提示符下输入：

```
Tracert 215.0.0.12
```

Tracert 命令可以很详细地跟踪连接到目标计算机 215.0.0.12 的路径信息，如中途经过多少次信息中转、每个中转花费了多少时间等，从而查出用户主机与远程计算机之间的线路故障等情况。

除了以上所介绍的这 5 个常用命令外，Microsoft 还在系统中内置了其他工具，如 Arp 命令用于显示并修改 Internet 到以太网的地址转换表；Nslookup 命令查询一台机器的 IP 地址和其对应的域名，它通常需要一台域名服务器来提供域名服务，如果用户已经设置好域名服务器，就可以用这个命令查看不同主机的 IP 地址对应的域名。

不同系统中的相应命令参数设置可能有不同之处，本书所列的这些工具软件参数用法是针对 Windows 操作系统，在 UNIX 和 Linux 中有很多不同。

9.4　网络连接设备的维护

不论是局域网、城域网还是广域网，其物理硬件通常都是由网卡、集线器、交换机、路由器、网线及 RJ-45 接头等网络连接设备和传输介质组成的。

9.4.1　网卡

网卡也叫网络适配器，是网络接口卡(Network Interface Card，NIC)的简称，是网络最基本的组成部分之一。它的主要作用是将计算机数据转换成能够通过介质传输的信号。现在使用的网卡大都是采用 PCI 接口的以太网卡，ISA 接口的网卡已基本被淘汰。

网卡在重启时能正常检测，但不能同其他机器互联。这种情况是子网掩码或 IP 地址配置错误、网线不通、网络协议安装不正确、路由器配置不正确等。解决方法是首先将 Ping 本网卡的回送地址(127.0.0.1)，若通则说明本机 TCP/IP 工作正常；若不通则需重新配置并重新启动计算机。有些网卡默认速率为 100Mb/s，也会导致网络不通，需要根据所连 Hub(集线器)或 Switch(交换机)口的速率，将其速率设置为 10Mb/s、100Mb/s 或设成自适应网线速率。

在搬动机器时网卡的损坏率往往较高。另外，主板上的 PCI 插槽有时也可能导致网卡出现问题。

9.4.2　集线器和交换机

交换机和集线器都是对网络进行延伸管理和扩展网络终端的重要设备。

集线器和交换机在网络结构中的作用是相同的，都是对网络进行集中管理的重要工具。只是集线器上的所有端口共享同一带宽，而交换机上的所有端口均有独享的信道带宽。

1. 交换机的定义

交换机是一种基于 MAC(网卡的硬件地址)识别，能完成封装转发数据包功能的网络设备。交换机可以“学习”MAC 地址，并将其存放在内部地址表中，通过在数据帧的始发者和目标接收者之间建立临时的交换路径，使数据帧直接由源地址到达目的地址。

2. 集线器的定义

集线器属于数据通信系统中的基础设备，它和双绞线等传输介质一样，是一种不需任何软件支持，或只需很少管理软件的硬件设备。集线器像网卡一样，应用于 OSI 参考模型第一层，因此又被称为物理层设备。集线器内部采用了电器互连，当维护 LAN 的环境是逻辑总线或环型结构时，完全可以用集线器建立一个物理上的星型或树型网络结构。在这方面，集线器所起的作用相当于多端口的中继器。其实，集线器实际上就是中继器的一种，其区别仅在于集线器能够提供更多的端口服务，所以集线器又叫多口中继器。

3. 交换机与集线器的区别

(1)　交换机与集线器的本质区别。用集线器组成的网络称为共享式网络，而用交换机组成的网络称为交换式网络。

共享式以太网存在的主要问题是所有用户共享带宽，每个用户的实际可用带宽随网络用户数的增加而递减。这是因为当信息繁忙时，多个用户可能同时“争用”一个信道，而一个信道在某一时刻只允许一个用户占用，所以大量的用户经常处于监测等待状态，致使信号传输时产生抖动、停滞或失真，严重影响了网络的性能。

(2)　在交换式以太网中，交换机提供给每个用户专用的信息通道，除非两个源端口企图同时将信息发往同一个目的端口；否则多个源端口与目的端口之间可同时进行通信而不会发生冲突。

通过实验测得，在多服务器组成的局域网中，处于半双工模式下的交换式以太网的实际最大传输速率是共享式网络的 1.7 倍，而工作在全双工状态下的交换式以太网的实际最大传输速率可达到共享式网络的 3.8 倍。

交换机只是在工作方式上与集线器不同，其他的如连接方式、速度选择等与集线器基本相同，目前的交换机同样从速度上分为 10Mb/s、100Mb/s 和 1000Mb/s 几种，所提供的端口数多为 8 口、16 口和 24 口几种。交换机在局域网中主要用于连接工作站、集线器、服务器或用于分散式主干网。

在实现小型企业局域网方案时，在并发用户不多、只作为一般办公应用的情况下可考虑使用组网经济、维护复杂程度低的集线器。但在网络较大，对网络速度要求较高的网络环境中或者在主干网络中就要考虑使用交换机。

4. 交换机与集线器的级联

集线器和交换机的性能优化主要体现在集线器或交换机的级联上。如果需要集线器与集线器或集线器与交换机级联，则一定要注意集线器的带宽是所有端口共享的，每个端口



的实际可利用带宽为总带宽除以所用端口数，所以一般不用集线器来级联，即使级联，也一般最多是两层，否则网络速度会呈倍差级数减慢。因此级联大多是通过用集线器连接在交换机的端口上实现的，因为交换机的带宽就是每个端口的实际可用带宽，而不受交换机所用端口数的限制。

交换机与带有级联口的集线器的级联方式是，用一条直通线通过集线器的级联口连接到交换机的任何一个端口(MDI-X)上。

(1) 交换机与没有级联口的集线器的级联方式。用直通线将交换机的级联端口(MDI)连接到集线器的任一端口。用交叉线将交换机的任一端口(MDI-X)与集线器的任意端口连接。

(2) 交换机与交换机的级联方式。用直通线将交换机的级联端口(MDI)连接到另一交换机的任一端口。用交叉线将交换机的任一端口(MDI-X)与另一交换机的任意端口连接。

集线器之间可通过面板上的 Up-Link 口级联，即将一台集线器的 Up-Link 口用直通线接到另一台集线器的任何一个 RJ-45 口上，也可将两个普通端口用交叉线连接来实现两个集线器的级联。

集线器的级联端口不能和其共用的端口同时使用。因为在集线器内部，级联端口与其共用端口实际上是同一端口，不可能同时连接两台设备。

9.4.3 路由器

路由器是多个网络或网段相连必不可少的网络设备。它能将不同类型网络的数据信息翻译成相互间能读懂的信息，从而组成更大的网络。

作为网络管理人员，配置路由器是一项重要的工作。一般路由器至少具备一个以太网口和一个同步口，在路由器面板上的指示分别为 LAN(以太端口)和 WAN(同步端口)。一台新买路由器的配置文件是空的，当为其进行简单的路由配置(包括这两个端口的配置和静态路由的添加)后，通过内部网交换机或集线器接到路由器以太网口上的工作站就可以通过同步端口与更远、更大的网络进行通信了，Internet 网就是这个道理。

在网络异常的情况下，可用“show interface 端口号”命令来查看链路的状态，借以判断以太网端口和同步端口是否有故障。

9.4.4 网线

网线有两种，一种是同轴电缆，另一种就是双绞线，同轴电缆基本已经淘汰，下面只对双绞线进行介绍。

双绞线是由不同颜色的 4 对 8 芯线组成，每两条按一定规则交织在一起，成为一个芯线对。作为以太局域网最基本的传输介质，双绞线习惯上称为网线。双绞线作为网络连接的传输介质，网络上的所有信息都需要在这样一个信道中传输，如果双绞线本身质量不好，传输速率受到限制，即使其他网络设备的性能再好传输速率再高也不行。

双绞线可分为屏蔽(Shielded Twisted-Pair，STP)与非屏蔽(Unshielded Twisted-Pair，UTP)双绞线两类，屏蔽的双绞线外面包有一层屏蔽用的金属膜，它的抗干扰性能要强于非屏蔽双绞线，大多数局域网使用非屏蔽双绞线作为布线的传输介质；单根网线由一定距离长的

双绞线与 RJ-45 头组成。

双绞线价格低廉、连接可靠、维护简单，可提供高达 1000Mb/s 的传输带宽，不仅可用于数据传输，而且还可以用于语音和多媒体传输。目前的超五类和六类非屏蔽双绞线可以轻松提供 155Mb/s 的通信带宽，并拥有升级至千兆的带宽潜力，因此，成为当今水平布线的首选线缆。

9.4.5　RJ-45 接头

RJ-45 接头又称为“水晶头”，是连接非屏蔽双绞线的连接器，为模块式插孔结构。RJ-45 接口前端有 8 个凹槽，简称 8P(Position)，凹槽内的金属接点共有 8 个，简称 8C(Contact)，因而也有 8P8C 的别称。

从侧面观察 RJ-45 接口，可以看到 8 片平行排列的金属片，每片金属片前端都有一个突出透明框的部分，从外表来看就是一个金属接点。按金属片的形状来划分，又有“二叉式 RJ-45”及“三叉式 RJ-45”接口之分。二叉式的金属片只有两个侧刀，三叉式的金属片则有 3 个侧刀。金属片的前端有一小部分穿出 RJ-45 的塑料外壳，形成与 RJ-45 插槽接触的金属脚。

在压接网线的过程中，金属片的侧刀必须刺入双绞线的线芯，并与线芯总的铜质导线内芯接触，以连通整个网络。一般地，叉数目越多，接触的面积也越大，导通的效果也越明显，因此三叉式的接口比二叉式接口更适合高速网络。

水晶头也有几种档次之分，有带屏蔽的也有不带屏蔽的，水晶头的质量得不到保证，会造成接触不良，网络不通。质量差的表现为塑料扣位不紧(通常是变形所致)，也很容易造成接触不良，网络中断。

9.5　网络性能优化

9.5.1　系统内存优化

1. BIOS 优化

BIOS 中与内存有关的选项在 BIOS 主界面的 Advanced Chipset Features 中，选项界面如图 9.4 所示。

以下介绍几个最常用的选项。如 CAS Latency，CL(CAS Latency)指的是内存存取数据所需的延迟时间，简单地说，就是内存接到 CPU 的指令后的反应速度。一般的参数值是 2 和 3 两种。CAS 延迟参数值越小，系统在读取 RAM 数据时的速度就越快。

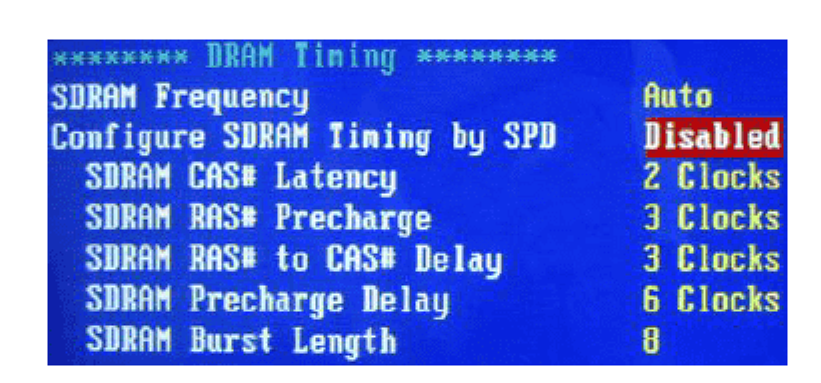


图 9.4　BIOS 中 Advanced Chipset Features 界面



SDRAM CAS 延迟值为 3，但基本上都可以达到 2。DDR 内存是双倍速率的 SDRAM(Dual date rate SDRSM)，是 SDRAM 的升级换代产品，它的数据传输速率为传统 SDRAM 的 2 倍，它的 CAS 延迟值一般设置为 2。RDRAM，它的 CAS 延迟要比 SDRAM 大得多，如果把 CAS 延迟设小一点效果非常显著。但改变 CAS 延迟实际上是一种超频，要注意它的稳定性(可以运行如 TimeDemo Loop 之类的稳定性测试软件)。

(1) RAS To CAS Delay，设置行激活命令到读/写命令之间的时间。这个值越小表示越快，在修改它时，也要注意系统的稳定性。

(2) RAS Precharge Time，设置 DRAM 预充电需要多少个周期的时间，值越小速度越快。在修改它的时候，同样要注意稳定性。

(3) SDRAM Precharge Control，设置系统如何管理 SDRAM 的预充电时间，它有两个值，即 Enabled 和 Disabled，在不同的系统上有不同的结果，建议两者都试一下。

(4) Shadow System BIOS，如果它为 Enabled 的话，在系统启动时会把 BIOS 中的内容复制到主内存中，对大多数机器来说，启动速度和运行速度都会加快。

(5) System BIOS Cacheable，当设为 Enabled 时，在必要时系统会把 BIOS 中的内容备份到 L2 缓存中，加快 BIOS 的运行速度，效果比 Shadow System BIOS 还要好。当 Shadow System BIOS 也设为 Enabled 时，效果最佳。

2. 注册表修改

在注册表中有若干个关于内存的设置，但在修改时要注意，因为稍有错误就会导致系统崩溃。所以在修改前要把注册表作一个备份，以备在出现问题恢复。

首先在注册表中找到 HKLM/System/CurrentControlSet/Control/Session Manager/Memory Management，会发现下面几个选项：

(1) DisableExecutivePaging，设为 Enabled 时， Windows 在运行可执行文件时不使用硬盘上的交换文件，这样操作系统和文件执行的速度会更快。推荐只有在系统内存大于 128MB 时，才将它设为 Enabled，因为它也要占用一定的系统资源。在默认状态下，它的值为 0(Disabled)，如果要为 Enabled 就为 1。

(2) LargeSystemCache，设为 Enabled 时(服务器版的 Windows 默认设置为 Enabled)，系统会把除了 4MB(作为硬盘缓存)以外的所有内存都用作文件系统的缓存。Windows 会把自己的内核放到内存中，这样运行起来就更快。这项设置是动态的，如果在某些情况下硬盘需要更多的缓存，系统会释放一些内存给硬盘作缓存。在默认情况下有 8MB 内存是留作此用途的。

此项设置的主要好处就是可以使操作系统运行得更快，并且它还是动态的，当内存需求不大时，Windows 的内核就驻留内存；如果运行多个程序需要大量内存，Windows 会把它的内核从内存中释放出来。0 表示 Disabled，1 表示 Enabled。不过如果把它设为 Enabled，系统会占用更多的内存，在一些任务很密集的情况下，系统性能会下降。根据 Microsoft 的说法，对那些自己进行缓存的应用程序如 Microsoft SQL，和需要大量内存才能得到最好性能的程序(如 IIS)来说，此项设置最好。

(3) IOPageLockLimit，这项设置主要是服务器应用。如果设置合理，在进行大数据量的文件传送和类似的操作时，可以提升系统的 I/O 性能。但是如果系统内存不足 128MB，

那么这项设置不会有任何作用。如果系统内存超过 128MB，可以把它设置为 8～16MB，性能的提升会比较明显。默认值是 0.5 MB(512 KB)。

3. 禁止启动时运行程序

禁止启动时运行一些不必要的程序可以少占用一些内存。在 Windows 2000 中禁止启动时运行程序不像 Windows 9x/Me 中那样简单，必须要修改注册表。注册表中相关的项为[HLKM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN]。找到之后，就可以进行修改了。不过还是要先做好备份，以防出现错误。

9.5.2　CPU 的优化

对于 CPU 的优化主要考虑 CPU 缓存技术和多处理器技术。

1. 缓存技术

目前使用的 CPU 都具有一个二级缓冲存储器(二级缓存)，主要用来保存 CPU 最近使用过的数据，为一级缓存传送数据提供方便。CPU 访问缓存的速度远远快于访问 RAM 的速度。

按照 CPU 结构的不同，二级缓存通常称为外部缓存，它的容量一般在 256 KB 到几兆之间。二级缓存是一个中转站，实现数据从物理内存到 CPU 的交换。由于 CPU 只能处理一级缓存中的数据，所以，二级缓存先将数据传递到一级缓存中，再由一级缓存传递到 CPU 进行处理。可见，CPU 的缓存越大，CPU 处理数据的速度就越快。

2. 多处理器技术

多处理器技术就是在一台计算机系统中安装多个 CPU，并协同处理数据。一个 CPU 一次只能执行一条指令，多个 CPU 的使用必将提高数据处理速度。不过，要实现多处理器技术需要支持多处理器安装的主板和操作系统。对于操作系统而言，Windows Server 是一个不错的选择，它支持 4～8 个 CPU，并使用对称式多处理器系统，可以将一个应用程序或服务中的进程由多个 CPU 来处理。

9.5.3　硬盘优化

对硬盘进行优化主要考虑硬盘的技术、硬盘的速度和文件系统。

1. 硬盘的技术

从当前的硬盘接口技术来看，硬盘主要分为两种，一种是 IDE 接口硬盘，另一种是 SCSI 接口硬盘。IDE 接口速度慢，但价格便宜，因此它广泛地应用于个人计算机和工作站。而 SCSI 接口是小型计算机系统接口的简称，它的设计要求传输速率高、支持多进程和并行处理。1988 年推出的 SCSI 标准使数据传速率提高到了 160Mb/s。早期的 SCSI 接口只用于小型机以上的高端计算机，现在已经有大量的中、低端服务器使用 SCSI 接口，而且开始出现在 PC 中。

IDE 与 SCSI 接口有很大的不同，首先是两者的接口方式不同，IDE 工作时需要 CPU 的全程参与，CPU 读写数据时就不能做其他事情，而 SCSI 接口则完全通过独立的高速 SCSI



控制卡来控制数据的读写操作，提高了系统的输入/输出处理能力，并能提供更多的 CPU 资源。就硬盘而言，IDE 接口硬盘对 CPU 的占用率一般要达到 30%～50%，而 SCSI 接口硬盘对 CPU 的占用率只有 4%～6%。虽然现在的 IDE 接口为了改善这些问题，在技术上也做了许多调整和改进，如应用 DMA 模式读写数据，但在一定程度上降低了对 CPU 的占用率，因此其性能仍无法与 SCSI 同日而语。另外，SCSI 接口的另一个特点是扩充性和安全性都非常好。一个 IDE 控制卡最多可以连接两个 IDE 接口设备，而一个 SCSI 控制卡最多可以连接 60 个 SCSI 接口设备。

由于 IDE 和 SCSI 接口硬盘在速度、容量、可靠性和稳定性等方面都有很大的差距，在选购时一定要根据需要来决定。一般地，PC 和网络中的工作站都使用 IDE 接口硬盘，而服务器主要使用 SCSI 接口硬盘。

2. 硬盘的速度

前面已经介绍过，SCSI 接口硬盘比 IDE 接口硬盘的速度要快得多，选择 SCSI 接口硬盘就等于选择高速硬盘。但是，由于价格或主板的原因只能选择 IDE 接口硬盘时，尽量选择高速的 IDE 接口硬盘。现在，IDE 接口硬盘主要有两种速度类型，一种是 5400r/s，另一种是 7200r/s。

3. 文件系统

文件系统就是在硬盘上存储信息的格式。在所有的计算机系统中，都存在一个相应的文件系统，它规定了计算机对文件和文件夹进行操作处理的各种标准和机制。因此，用户对所有的文件和文件夹的操作都是通过文件系统来完成的。其中，Windows 支持的文件系统包括以下几种。

(1) FAT。标准文件分配表，运行在 Windows NT、Windows 95、MS-DOS 或 OS/2 上，可以存取主分区或者逻辑分区上的文件。FAT 文件系统是一种最初设计用于小型磁盘和简单文件结构的简单文件系统。采用 FAT 文件系统格式化的卷以簇的形式进行分配，默认的簇大小由卷的大小决定。对于 FAT 文件系统，簇的数目必须可以用 16 位的二进制数字表示，并且是 2 的乘方。由于额外开销的原因，在大于 511MB 的卷中不推荐使用 FAT 文件系统。如果用户的计算机上运行的是 Windows 95、Windows for Workgroups、MS-DOS、OS/2 或 Windows 95 以前的版本，那么 FAT 文件系统格式是最佳的选择。不过，需要注意的是，FAT 文件系统最好用在较小的卷上。因为，在不考虑簇大小的情况下，使用 FAT 文件系统，则卷不能大于 4GB。

(2) FAT32。增强的文件分配表，它是在大型磁盘驱动器(超过 512MB)上存储文件的极有效的系统。FAT32 文件系统提供了比 FAT 文件系统更为先进的文件管理特性，如支持超过 32GB 的卷以及通过使用更小的簇来更有效率地使用磁盘空间。作为 FAT 文件系统的增强版本，它可以在容量从 512MB 到 2TB 的驱动器上使用。在以前的操作系统中，只有 Windows2000、Windows 98 和 Windows 95 OEM Release 2 版能够访问 FAT32 卷。MS-DOS、Windows 3.1 及较早的版本、Windows for Workgroups、Windows NT 4.0 及更早的版本都不能识别 FAT32 卷，同时，也不能从 FAT32 上启动它们。

(3) NTFS。只有运行 Windows 2000、Windows NT 和最新的 Windows XP 的计算机才可以存取 NTFS 卷中的文件。NTFS 文件系统提供了 FAT 和 FAT32 文件系统所没有的读写

能力、可靠性和兼容性。NTFS 文件系统的设计目标就是用来在很大的硬盘上很快地执行诸如读、写和搜索这样的标准文件操作，甚至包括像文件系统恢复这样的高级操作。NTFS 文件系统包括公司环境中文件服务器和高端个人计算机所需的安全特性。NTFS 文件系统还支持对于关键数据完整性十分重要的数据访问控制和私有权限。除了可以赋予 Windows 计算机中的共享文件夹特定权限外，NTFS 文件和文件夹无论共享与否都可以赋予权限。NTFS 是 Windows 中唯一允许为单个文件指定权限的文件系统。然而，当用户从 NTFS 卷移动或复制文件到 FAT 卷时，NTFS 文件系统权限和其他特有属性将会丢失。

从上面的内容可以看出，无论是网络用户还是个人用户最好都使用 NTFS 文件系统。不过，如果网络用户需要配置多重启动(包括 Windows 98 等不支持 NTFS 文件系统的操作系统)，可以使用 FAT32 文件系统。如果个人用户没有使用 Windows 等支持 NTFS 文件系统的操作系统，也最好使用 FAT32 文件系统。当然，如果用户的系统中仍安装着 Windows NT 等低端操作系统，则需要使用至少一个 FAT 分区。

9.5.4　网络接口优化

网络接口性能的调整和优化不仅涉及网络数据的进出问题，而且关系到整个网络的服务、设备和布线等网络构成问题。选择高性能的网卡和驱动程序，并配置好网络服务和协议，可以大大提高网络的传输速度和稳定性。

1. 网卡和驱动程序的选择

网卡承担的任务是非常繁琐的，它要从网络中接收数据包，先确认是否属于本地计算机，接收后要发送到 CPU 进行处理，并尽可能地保证数据的传输速度。另外，一些网卡与软件结合起来，可以使用客户端或服务器端的管理特性对网络中的计算机运行情况进行监视。在选择网卡时，除了考虑网络的综合性能外，还要考虑网卡的数据吞吐能力，在网络计算机硬件系统允许的情况下应尽量选择高速网卡。对于工作站，应选择 10Mb/s 或 100Mb/s 的网卡，对于服务器应选择 100Mb/s 或 1000Mb/s 的网卡。如果经济条件允许，可以选择一些专门为服务器设计的网卡，它们能够最大限度地降低对服务器 CPU 的占用率，优化了服务器的性能。

由于 Windows 等网络操作系统的硬件兼容性都比较好，大部分网卡在安装到系统后都不需要用户手动安装驱动程序即可使用。但是，系统默认的驱动程序大都只能驱动网卡，不能保证网卡发挥最佳性能。所以，建议用户为网卡安装专门配置的驱动程序或最新的驱动程序。

2. 服务和协议的设置

在为网卡设置服务组件时，要了解网络的工作特点，根据情况选择要使用的网络组件，不可一味地将所有的网络组件添加到系统中，这样会严重影响网络的性能。因为这些网络组件的功能在系统启动时都会自动加载，不但占用大量的系统资源，而且能对网络的正常通信产生干扰。

同其他网络组件一样，安装不必要的网络协议也会影响网络的性能。对于一般的网络，只需使用 TCP/IP 协议即可。如果需要连接其他计算机系统，可以选择相应的协议。例如，



要连接 NetWare 网络，可以添加 IPX/SPX 协议。另外，协议与网络的绑定顺序也需要考虑。管理员应将主要的网络协议放在绑定顺序的最前面。例如，在网络中使用 TCP/IP 协议进行网络连接和数据传送的机会比利用 IPX/SPX 协议进行连接和数据传送多时，可以将 TCP/IP 协议放置在绑定顺序的首要位置。

9.6 网络故障和排除

网络和单机最大的不同是牵一发而动全身，一台单机上的问题很可能映射到网络中的某个环节，甚至破坏全部的网络运转。本节针对网络故障进行介绍，并介绍故障排除的思路和方法。

9.6.1 网络常见故障概述

引起网络出现故障的因素有多种，但总的来说可以分为硬件故障和软件故障两大类。下面简单介绍常见的硬件和软件故障种类。

表 9.1 列出了常见的硬件故障，实际的网络统计结果表明，硬件问题中出现最多的是网线制作方法不当或网线接头处制作不良。这些问题看似简单却最容易出问题，在网络故障检查时应列为首先检查的对象。

表 9.1 硬件故障

故障种类	原 因
设备本身问题	网线接头制作不良；网线接头部位或中间线路部位有断线
	网卡质量不良或有故障；网卡和主板 PCI 插槽没有插牢，从而导致接触不良：网卡和网线的接口存在问题
	集线器质量不良；集线器供电不良；集线器和网线的接口接触不良
	交换机质量不良；交换机和网线接触不良；交换机供电不良
设备之间问题	网卡和网卡之间发生中断请求和 I/O 地址冲突
	网卡和显卡之间发生中断请求和 I/O 地址冲突
	网卡和声卡之间发生中断请求和 I/O 地址冲突

软件安装或设置不当引起网络故障方面的情况见表 9.2。

表 9.2 软件问题

故障种类	原 因
设备驱动程序方面的问题	驱动程序和操作系统不兼容
	驱动程序之间的资源冲突
	驱动程序和主板 BIOS 程序不兼容
	设备驱动程序没有安装好，引起设备不能正常工作
网络协议方面的问题	没有安装相关网络协议
	网络协议和网卡绑定不当
	网络协议的具体设置不当

续表

故障种类	原　因
相关网络服务方面的问题	相关网络服务方面的问题主要指的是在 Windows 操作系统中共享文件和打印机方面的服务，即要安装 Microsoft 文件和打印共享服务
网络用户方面的问题	在对等网中，只需使用系统默认的 Microsoft 友好登录即可，但是若要登录 Windows NT 域，就需要安装 Microsoft 网络用户
网络表示方面的问题	在 Windows 98/2000 和 XP 中，甚至是在 NT 或者 2000 的域中，如果没有正确设置用户计算机在网络中的网络标识，很可能会导致用户之间不能相互访问
其他问题	这些问题和用户的设置无关，但和用户的某些操作有关，如大量用户访问网络会造成网络拥挤甚至阻塞、用户使用某些网络密集型程序造成的网络阻塞

由软件设置引起的局域网不通的问题中，最常见的是 TCP/IP 协议中的 IP 地址设置不当导致的网络不通，其次是网络标识不当引起的相互之间无法访问。

9.6.2　网络故障排除的思路

引起网络不通的因素有很多种，如果面对故障现象茫然无措，会在解决网络问题时浪费大量的时间和精力，所以需要按照一定的思路和方法来对故障原因进行一一排除，最后将故障原因准确定位，从而在解决网络问题时事半功倍。

具体排除思路是先询问、观察故障时间和原因，然后动手检查硬件和软件设置，而动手(观察和检查)则要遵循先外(网间连线)后内(单机内部)、先硬(硬件)后软(软件)的次序。由于目前使用星型网络的情况最多，在此以星型网络为例介绍网络故障的排除思路。具体来说，排除网络故障时应该按照以下顺序来进行。

(1)　询问。应该询问用户最后一次网络正常的时间，从上次正常到这次故障之间机器的硬件和软件都有过什么变化与进行过哪些操作，是否是由于用户的操作不当引起网络故障，根据这些信息快速地判断故障的可能所在。因为有很多网络问题实际上和网络硬件本身没有什么关系，大多数是由于网络用户对计算机进行误操作造成的。用户极有可能安装了会引起问题的软件、误删除了重要文件或改动了计算机的设置，这些都很有可能引起网络故障，对于这些故障只需进行一些简单的设置或者恢复工作即可解决。如果网络中有硬件设备被动过，就需要检查被动过的硬件设备。例如，若网线被换过，就需要检查网线类型是否正确，PC 到集线器或交换机应使用直通线，而不是级联交叉线或反转线。

(2)　检查。上述询问工作完成后，就需要进行相关事项的检查，检查验证网络物理设备是否工作正常。排除故障应该先排除物理层的因素，也就是要先排除网线、网线接头、集线器或交换机的物理故障因素。如果这些因素不排除，而先从网卡方面或协议设置上找原因尝试修改设置，很有可能原来的故障没有解决，反而造成新的人为故障。

①　首先要检查共同的通道。例如，检查使用相同集线器或交换机的计算机网络是否正常。如果都不正常，则可能是集线器或交换机故障，如果其他都正常只有故障机不正常，



则可以先从正常机上拔下网线，给故障机使用，检查它是否正常。如果正常，说明可能是故障机所连接的集线器或交换机口故障，但是这种可能性较小，很有可能是网线故障，此时可以使用万用表检测网线的连通性，如果网线不通，可以使用压线钳重新压紧水晶头或者剪掉原来的水晶头重新制作。如果网线正常，说明集线器或交换机的端口有问题。大多数的网络故障都是由物理层的故障引起的。

② 如果检查了网络的物理层后，没有发现问题，那么接下来就要进行网络的数据链路层的检查。数据链路层涉及的设备有网卡和交换机。对于网卡，需要检查其工作状态与设置参数是否正常；对于交换机，如果是有设置的交换机，就需要验证交换机设置的正确性，因为极有可能是有人将交换机的设置做了错误的修改，导致交换机的部分端口不能正常工作，从而导致网络出现故障。

每个网卡都有其确定的设置参数，容易出现问题的地方是网卡“中断请求”(IRQ)设置、基本 I/O 端口地址和存储器地址。如果这些方面出现任何差错，或与工作站或终端中其他设备产生冲突，NIC 即使能工作，也无法连续工作。一般情况下，计算机有 16 个 IRQ 号。将这些 IRQ 号分配给不同设备，如表 9.3 所示。在设备发出中断请求时，就可向处理器发出中断请求信号。I/O 端口地址作为处理器和设备之间所有信息传输的通道。

表 9.3　IRQ 号与设备对应表

IRQ 号码	设备类型
00	系统计时器
01	键盘
02	可编程中断控制器
03	通信端口 2 或 4
04	通信端口 1 或 3
05	打印机端口 2(LPT2)或开放
06	软盘控制器
07	打印机端口 1(LPTI)
08	实时时钟
09	从 IRQ 重定向或开放
10	开放
11	开放
12	PS/2 标端口或开放
13	算术协处理器
14	IDE 硬盘驱动器控制器
15	IDE 硬盘驱动器控制器或开放

③ 如果检查了网络的数据链路层后，没有发现问题，接下来就需要检查网络层和传输层。

首先要验证是否正确设置 TCP/IP 协议，诸如 IP 地址、子网掩码、默认网关、DNS、WINS 设置等的正确性都需要验证，因为这些参数都极有可能被他人误修改。

验证网络协议是否被正确加载，这需要到 DOS 的 COMMAND 窗口下输入“Ping 127.0.0.1”，如果 Ping 不通，则需要卸载 TCP/IP 协议，然后重新安装设置；如果返回正确的测试结果，如图 9.5 所示，则表明 TCP/IP 协议被正确加载。

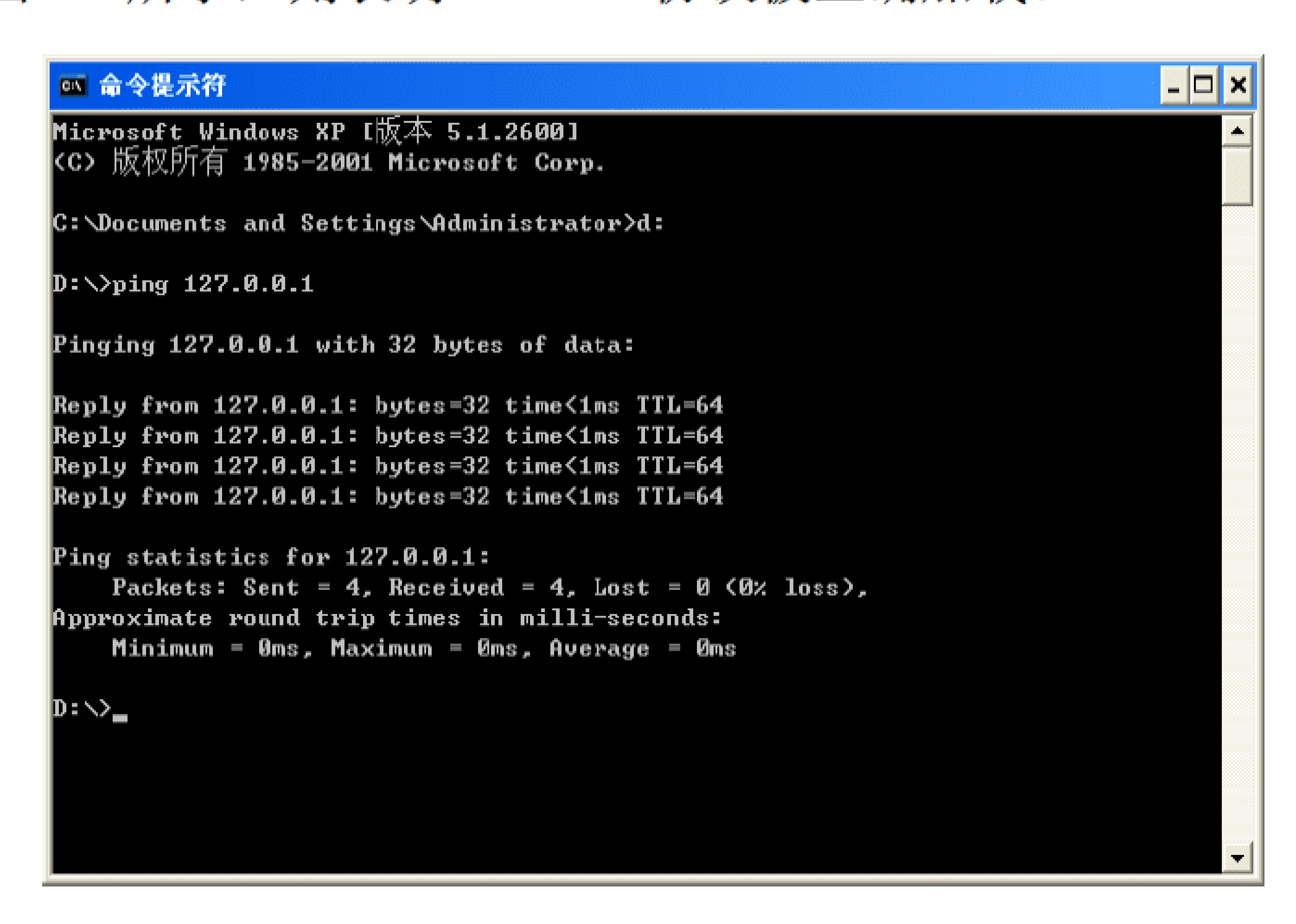


图 9.5 返回正确的测试结果

接下来需要使用 Ping 验证网关是否能连通，如果网关不能连通则表明本地链路方面有故障，网关如果能 Ping 通，则需要进一步 Ping 目的计算机的 IP 地址，如果 Ping 不通的话，则可能是目的计算机未开机或目的计算机链路方面有网络故障。

④ 如果目的计算机能 Ping 通，但是网络应用层的程序却不能连通，则需要检查防火墙的参数设置与加载的设置是否正确，还需要检查相关网络应用程序的参数设置是否正确。

上述的故障排除方法也适用于交换机、路由器之类的网络硬件设备的故障排除，只是路由器级别的网络硬件设备故障排除需要涉及更多的故障排除方法与手段。但无论哪一方面网络故障的排除，都需要用户对网络基础知识进行全面、正确的掌握，这将有助于正确、快速地排除网络故障。

由于 PCI 的设备都支持 PNP 功能，因此 PCI 设备可以自动检测并设置没有使用的中断与地址，所以一般不会出现中断与地址的冲突。冲突往往发生在同时使用 PCI 与 ISA 设备的机器中，这时需要在 CMOS 中为 ISA 设备设置并保留其预设的中断与地址，然后让 PCI 设备自己检测并设置自己的中断与地址。当然也可以使用 ISA 设备自带的设置程序进行中断与地址的修改。

127.0.01 的 IP 地址被规定为环路测试地址(Loop Back)，目标地址为 127.0.0.1 的包不会被送到本机上的网络设备，而是被送到本机的 Loop back 驱动器上去。此 IP 地址用来检测 TCP/IP 协议组是否正常工作。

9.6.3 局域网故障与排除

1. 局域网网络故障判断

局域网在构建和使用时，难免出现故障。排除故障、优化系统是管理局域网最基本的工作之一。在此从排除故障、优化性能的角度出发，简单归纳了一些局域网维护及优化的经验和技巧，其中着重讨论了网卡、网线的正确安装、合理设置等问题。了解这些，有助



于更好地去维护计算机、管理网络，从而更好地利用网络去开展工作。

1) 有故障时先查网卡

在局域网中，遇到网络不通时，首先认真检查各连入网络的机器中网卡设置是否正常。检查时，可以用鼠标依次打开【控制面板】|【系统】|【设备管理】|【网络适配器】设置窗口，在该窗口中检查一下有无中断号及I/O地址冲突(最好将各台机器的中断设为相同，以便对比)，直到网络适配器的属性中出现【该设备运转正常】，并且在【网上邻居】中至少能找到自己，说明网卡的配置没有问题。

2) 确认网线和网络设备工作正常

当检查网卡没有问题时，此时可以通过网上邻居来查看网络中的其他计算机，如果还不能看到网络中的其他机器，说明可能是由于网络连线中断。网络连线故障通常包括网络线内部断裂，双绞线、RJ-45水晶头接触不良，或者是网络连接设备本身质量有问题，或是连接有问题。这时，可以使用测线仪来检测一下线路是否断裂，然后用替代法来测试一下网络设备的质量是否有问题。在网线和网卡本身都没有问题的情况下，再看一看是否软件设置方面的原因，如果中断号不正确也有可能导致故障出现。

3) 检查驱动程序是否完好

对硬件进行了检查和确认后，再检查驱动程序本身是否损坏，如果没有损坏，看看安装是否正确。如果这些可以判断正常，设备也没有冲突，就是不能连入网络，这时可以将网络适配器在系统配置中删除，然后重新启动计算机，系统就会检测到新硬件的存在，然后自动寻找驱动程序再进行安装。

4) 正确对网卡进行设置

在确定网络介质没有问题但还是不能接通的情况下，再返回网卡设置中，看看是否有设备资源冲突，有许多时候冲突也不是都有提示的。

为解决这种设备的冲突，可以按照以下操作步骤来进行设置，首先在设置窗口中将COM2屏蔽，并强行将网卡中断设置为3；如果遇到PCI接口的网卡和显卡发生冲突时，可以采用不分配IRQ给显卡的办法来解决，就是将CMOS中的 Assign IRQ for VGA 一项设置为“Disable”。

5) 禁用网卡的PnP功能

有的网卡虽然支持PnP功能，但安装好后发现并不能好好地工作，甚至不能工作。为此，可以采用屏蔽网卡的PnP功能的方法来解决这一故障。要想禁用网卡的PnP功能，就必须运行网卡的设置程序(一般在驱动程序包中)。在启动设置程序后，进入设置菜单。禁用网卡的PnP功能，并将可以设置的IRQ一项修改为一个固定的值。保存该设置并退出设置程序，这样如果没有其他的设备占用该IRQ，可以保证不会出现IRQ冲突。

另外，如果要安装Windows 98/2000/XP操作系统，必须保证操作系统不会将对应的中断类型作为具有PnP功能的IRQ进行处理，所以要在CMOS中将该中断的类型由PCI/ISA PnP修改为Legacy ISA。使用该方法可以解决大多数PnP网卡的设备冲突问题，但不一定对所有的PCI网卡都有效，因为有些网卡的设置程序根本就不提供禁用PnP功能选项。

6) 合理设置服务器的硬盘

使用局域网办公的用户，经常会使用网络来打印材料和访问文件。由于某种原因，网络访问的速度可能会不正常，这时往往会错误地认为导致网速降低的原因可能是网络中的

某些设备发生了瓶颈，如网卡、交换机、集线器等，其实对网速影响最大的还是服务器硬盘的速度。因此正确地配置好局域网中服务器的硬盘，将对整个局域网中的网络性能有很大的改善。通常，在设置硬盘时需要考虑以下几个因素。

(1) 服务器中的硬盘应尽量选择转速快、容量大的，因为硬盘转速快，通过网络访问服务器上的数据的速度也越快。

(2) 服务器中的硬盘接口最好是 SCSI 型号的，因为该接口比 IDE 或 EIDE 接口传输数据时速度要快，它采用并行传输数据的模式来发送和接收数据。在同一 SCSI 通道，不要将低速 SCSI 设备(如 CD)与硬盘共用，否则硬盘的 SCSI 接口高速传输数据的性能将得不到发挥。

(3) 如果条件允许，可以给网络服务器安装硬盘阵列卡，因为硬盘阵列卡能较大幅度地提升硬盘的读写性能和安全性。

7) 按规则进行连线

连接局域网中的每台计算机都是用双绞线来实现的，但并不是用双绞线把两台计算机简单地相互连接起来就能实现通信目的，而是必须按照一定的连线规则来进行连线。双绞线的连接距离不能超过 100m，如果需要连接超过 100m 的两台计算机时，必须使用转换设备。

在连接转换设备和交换机时，还必须进行跳线。这是因为以太网中，一般是使用两对双绞线，排列在 1、2、3、6 的位置，如果使用的不是两对线，而是将原配对使用的线分开使用，就会产生较大的串扰，对网络性能造成较大影响。10Mb/s 网络环境这种情况不明显，100Mb/s 的网络环境下如果流量大或者距离长，网络就会无法联通。

8) 严格执行接地要求

由于在局域网中，传输的都是一些弱信号，如果操作稍有不当或者没有按照网络设备的具体操作要求来办，就可能在联网中出现干扰信息，严重的可能导致整个网络不通；特别是一些网络转接设备，由于涉及远程线路，因此对接地的要求非常严格，否则该网络设备将达不到规定的连接速率，从而在联网的过程中产生各种莫名其妙的故障现象，给工作带来很大的麻烦。

9) 使用质量好、速度快的新式网卡

局域网中出现的故障大部分与网卡有关，或者是网卡没有正确安装好，或者是网络线接触不良，也有可能是网卡比较旧，不能被计算机正确识别，另外也有的网卡安装在服务器中，经受不住大容量数据的冲击，最终报废等。

因此，为避免上述的现象发生，一定要舍得投资，如果网卡是安装在服务器中，一定要使用质量好的网卡，因为服务器一般都是不间断运行，只有质量好的网卡才能长时间进行“工作”。另外，由于服务器传输数据的容量较大，因此购买的网卡容量必须与之匹配，这样才能实现“好马配好鞍”。

2. 局域网常见的故障排除概述

出现局域网故障不要慌张，只要按照系统的层次化结构来进行排除，一层一层解决，检查完服务器再检查客户端，就一定能够找出问题的原因并加以解决。



1) 故障检测第一步 Ping

Ping 命令在网络故障排除中是非常有用的一个工具，往往作为网络管理员探测故障原因的首选。当 Ping 一台主机时实际上是向那台主机发出了一个 ICMP 数据包，而 ICMP 协议又是在 TCP/IP 协议中的第二层 Internet 层。当一台客户端无法享受服务器提供的服务时，可以首先试着 Ping 一下服务器的 IP 地址，如果能够 Ping 通，而且没有丢包现象，那么就可以确定 Internet 以及它以下的各层都是没有问题的，这样就可以将检测问题的主要精力放在应用层，试着去找出其中的问题所在。

如果 Ping 不通或 Ping 通了但有丢包现象，那么就可以先将问题锁定在 Internet 层和网络接口层，首先解决这两层的问题，再看上层是否有问题。

2) 网络接口层故障排除

当出现网络故障时，可以在客户端首先使用 Ping 命令，Ping 服务器的 IP 地址，如果 Ping 通，证明故障肯定不在网络接口层，如果 Ping 不通或 Ping 通了但有丢包现象，问题可能出现在网络接口层或 Internet 层，但根据层次结构，首先应该检查的还是网络接口层，首先排除了网络接口层的问题后，再进行后续的检查，网络接口层最有可能出现问题的地方是网线、集线器、网卡、交换机，检测时按照此顺序进行。

3) 网线问题

网络中的计算机互相连接都需要网线，而网线也处在整个层次结构中的最低层，也是最容易出问题的地方。因此必须首先了解网线的种类以及连接设备使用网线的情况后，才可以排除网线的故障。

4) 网线种类

(1) 直通缆(标准 568B)。两端线序一样，线序是：白橙，橙，白绿，蓝，白蓝，绿，白棕，棕。

(2) 交叉缆(标准 568A)。一端为直通缆的线序，另一端为：白绿，绿，白橙，蓝，白蓝，橙，白棕，棕。

5) 设备连接使用网线情况

(1) PC-PC：交叉缆。

(2) PC-Hub：直通缆。

(3) Hub-Hub 普通口：交叉缆。

(4) Hub-Hub 级联口-级联口：交叉缆。

(5) Hub-Hub 普通口-级联口：直通缆。

(6) Hub-SWITCH：交叉缆。

(7) Hub-级联口 SWITCH：直通缆。

(8) SWITCH-SWITCH：交叉缆。

(9) SWITCH-ROUTER：直通缆。

(10) ROUTER-ROUTER：交叉缆。

(11) 100Base-T 连接双绞线，以 100Mb/s 的 EIA/TIA 568B 作为标准规格。

3. 常见网络故障及排除

1) 网线问题

(1) 网线用错。

故障原因：通过上面的讲解得知直通缆和交叉缆在不同设备之间的应用，如果安装线

缆或布线的时候用错网线就会导致网络不通。

查找方法：如果网线裸露在外，只要把网线的两头对在一起就能很容易发现此网线是直通缆还是交叉缆。如果网线已经布好就需要测线仪来进行测量了。

解决方法：发现网线用错了就换一根对的网线，如果布好的网线用错了，就需要将某一头接一根转接线或转接头，将错误的网线转换成正确的线序。

(2)　网线折断。

故障原因：当网络不通时，有可能是网线折断或接触不良。

查找方法：用电缆/光缆测试仪测量电缆或光缆的连通状况和属性的其他信息。

数字万用表：测量经过电缆的电脉冲，确定电缆是否有短路或断路。

时域反射器(TDR)：可利用声脉冲找出电缆的断点位置。

解决方案：找到折断的网线，将此网线替换。

2)　集线器问题

如果通过上面的检测，证明连接客户端和服务器的网线没有问题，那么下一个检测目标就会锁定在集线器上。集线器的作用是把网线集中连接在一起，所以如果集线器有问题网络自然也就不会通畅。

集线器损坏。

故障原因：当集线器损坏时，连接在集线器上的所有计算机都无法进行通信。

查找方法：确保网线没有问题后，如果客户端还 Ping 不通服务器，首先测试其客户端是否能够 Ping 通服务器，如果其客户端能够 Ping 通服务器，证明集线器没有问题，如果 Ping 不通证明问题也许出在集线器。再测试连接在此集线器上的其他客户端是否能够互相 Ping 通，如果能够 Ping 通，证明此集线器没有问题，问题可能出在其他方面。如果其他客户端都彼此 Ping 不通，那么证明问题就出现在本地集线器。

解决方案：如果确定是集线器的问题，解决方案就是更换一个好的集线器。

故障原因：当集线器的某个端口损坏，此端口连接的计算机就无法与其他计算机通信了。

查找方法：如果通过上面的方法证明集线器没有损坏，但本地客户端还是无法 Ping 通服务器，就可以尝试使用其客户端 Ping 本地客户端，如果集线器上所有其他客户端都能够互相 Ping 通，而他们却都无法连接到本地客户端，而本地客户端也连接不到其任何一台机器，就可以证明是此计算机连接到的集线器的端口损坏或接触不良。

解决方案：找到此计算机在集线器上的网络连线，重新插好，如果故障依旧存在，就可将此计算机的网络连线换一个端口，或更换一个集线器。

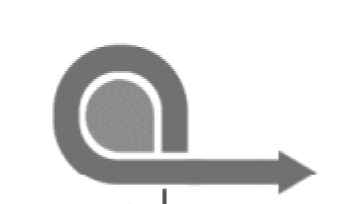
3)　网卡问题

如果通过上面的测试，证明网线和集线器都没有问题，那么下一个需要测试的对象就是网卡。网卡是网络接口层的另一个核心组件，不论是服务器还是客户端的网卡损坏，损坏任意一端的计算机都无法发送和接收任何信息。

(1)　网卡端口接触不良。

故障原因：客户端或服务器的网卡端口接触不好，所以有一方无法进行通信。

查找方法：确定网线、集线器都没有问题后，如果客户端还 Ping 不通服务器，首先测试本地客户端的网卡，再测试服务器的网卡。首先在客户端上确定其 IP 地址设置没有问题，



然后重新插一下连接的网线，查看其他计算机能否 Ping 通本地客户端，如果可以，再用本地客户端 Ping 服务器，如果成功证明客户端的网卡有问题。

如果通过前面的实验发现本地客户端能够与其他计算机通信，问题就有可能出现在服务器。首先确定服务器的 IP 地址配置正确，然后重新插一下连接的网线，查看其他计算机能否 Ping 通服务器，如果通信成功，证明服务器的网卡有问题。

解决方案：重新插拔一下连接的网线。

(2) 网卡损坏。

故障原因：如果网卡的芯片损坏，网络中的计算机自然就无法通信。

查找方法：如果通过上面的方法，重新插拔网卡后问题依旧存在，首先在客户端上确定其 IP 地址配置没问题，然后更换一块网卡，查看其他计算机能否 Ping 通本地客户端，如果可以再用本地客户端 Ping 服务器，如果成功证明客户端的网卡芯片有问题。

如果通过前面的实验发现本地客户端能够与其他计算机通信，问题就有可能出在服务器。首先确定服务器的 IP 地址配置正确，然后更换一块网卡， 查看其他计算机能否 Ping 通服务器，如果通信成功，证明服务器的网卡有问题。

解决方案：更换网卡。

4) 交换机问题

在现在的网络中，集线器往往被交换机替代，这样虽然增加成本，但是网络的整体性能会有很大提升。出于节省成本考虑，集线器之间也可以通过交换机来连接，这样通信速度有所提高，而且也不会增加太多成本。所以一旦交换机出现问题，查找和处理起来要比集线器复杂得多。

(1) 交换机 MAC 地址列表有问题。

故障原因：交换机是通过内置的 MAC 地址列表来帮助计算机之间通信的，所以一旦 MAC 地址列表出现问题，很有可能该收到数据的计算机收不到，不该收到信息的计算机可能会收到，而且也会产生丢包现象。

查找方法：通过 Windows 内置的 Network Monitor 来检测是否能够收到不该收到的信息。

【例 9.7】 选择 3 台计算机，一台作为 FTP 服务器，另一台作为 FTP 客户端，第三台作为监视客户端。

步骤如下：

① 首先配置好 FTP 服务器和客户端，然后在监视客户端上打开【添加删除程序】对话框，在【添加删除 Windows 组件】中选择【管理和监视程序】来安装网络监视器，在监视客户端上启动网络监视器。

② 转到 FTP 客户端，以用户“administrator”连接 FTP 服务器。

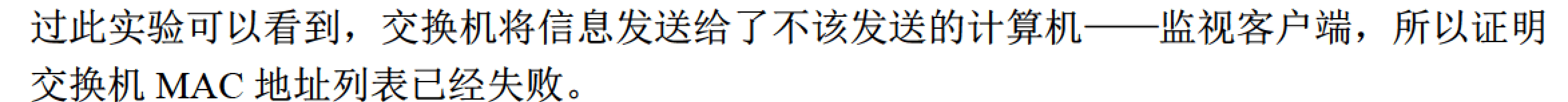
③ 回到监视客户端，停止并显示捕获的数据。

④ 选中【显示】，“筛选程序”对捕获到的数据进行筛选。

⑤ 只显示 FTP 和 Telnet 协议数据，单击【确定】按钮。

⑥ 捕获结果，通过查找 FTP 协议，可以发现 Pass 后面就是刚才访问 FTP 服务器用户 administrator 的密码“123456”。

交换机应该通过其 MAC 地址列表，将通信传输限制在 FTP 客户端和服务器之间。通



过此实验可以看到，交换机将信息发送给了不该发送的计算机——监视客户端，所以证明交换机 MAC 地址列表已经失败。

解决方案：重新启动交换机，如果还是解决不了，就更换交换机。

(2) 交换机损坏。

故障原因：交换机整个损坏。

查找方法：跟集线器的查找方法一样。

解决方案：更换交换机。

5) Internet 层和传输层故障排除

如果通过上述方法测试，发现网线、集线器、网卡、交换机都没有问题，就可以将问题检测提到解决方案 Internet 层和传输层。

(1) IP 地址冲突。

故障原因：如果在网络中发生两台计算机使用一个 IP 地址的情况，那么这两台计算机启动后，有一台计算机是可以进行正常通信的，而另一台则不行。

查找方法：如果一台计算机 IP 地址已经配置，但不能跟其他计算机通信。

需要利用 Ipconfig 工具查看其 IP 地址的真实运行状况。其真正的 IP 地址为 0.0.0.0，说明这台计算机上配置的 IP 地址正与其他计算机的地址发生冲突。

如果此计算机的 IP 地址是合法的，那么证明其他计算机在制作恶意冲突。可以在其他计算机上用 Netstat 命令查找计算机。在其他正常运行的计算机上输入 Netstat -a 冲突的 IP 地址，就可以找到恶意冲突的计算机。

解决方案：将其中一台计算机另外配置一个合法的 IP 地址。

(2) IP 地址配置问题。

故障原因：IP 地址配置不符合网段的配置要求，也会造成不能跟其他计算机通信的故障。

查找方法：如果通过 Ipconfig 发现本机的 IP 地址并没有出现 0.0.0.0 冲突现象，可以检查是否是 IP 地址配置问题。首先确定本网段的 IP 地址范围，如 192.168.1.0。然后在客户机上再次运行 Ipconfig 工具，查看其 IP 地址是否是本网段的 IP 地址，如果不是则修改本地计算机的 IP 地址。

解决方案：如果计算机使用静态的 IP 地址，就由网络管理员来为此计算机重新配置合法的本网段的 IP 地址。如果计算机是 DHCP 客户端，就在此计算机上运行 Ipconfig/Release 命令来释放原有的地址，再运行 Ipconfig/Renew 重新获得合法的 IP 地址。

(3) 路由器问题。

故障原因：本地的 IP 地址配置正确，服务器的 IP 地址配置也正确，但因为它们不在同一个网段，所以需要路由器来传递信息，如果路由器出现问题，客户端与服务器一样不能通信。

查找方法：在确定服务器和客户端双方的 IP 地址配置都没有问题后，首先使用 Ping 命令查找主机，主机没有回应。

解决方案：联系路由器管理员，重新配置路由器的信息。

6) 应用层故障排除

应用层的故障可谓千奇百怪，因为应用层的软件与服务器有成千上万种，所以可能出



现的问题也就非常多。在这里不可能将所有的问题一一列举出来，所以在这部分重点来解决 Windows 中各种服务容易出现的问题。

(1) DHCP 故障排除。

DHCP 故障虽然是在应用层的服务，但实质却是分配 IP 地址，所以错误往往影响的是 Internet 层，也就是 IP 地址故障。DHCP 大多数的故障现象就是配置好客户端和服务器后却发现客户端不能获得 IP 地址。但引起故障现象的原因却可能有很多种。

(2) 授权问题。

故障原因：DHCP 服务器需要经过授权后才能启动服务，所以如果未经授权服务器是不能分配 IP 地址的。

解决方案：如果发现 DHCP 服务器未经授权，就必须使用管理员身份打开 DHCP 服务器控制台进行授权操作。

(3) 服务器端 IP 地址问题。

故障原因：检查服务器已经经过授权，而且作用域已经被激活。这时应该检查作用域的地址范围是否与 DHCP 服务器的 IP 地址属于一个地址范围。如果 DHCP 服务器的 IP 地址与作用域的地址不在同一个网段内，DHCP 服务器也是不能分配 IP 地址的。

解决方案：将 DHCP 服务器的 IP 地址改为与作用域在同一个网段。

(4) 客户端配置问题。

故障原因： DHCP 分配出的地址与网络中的其他计算机有冲突，在客户端上显示 IP 地址为 0.0.0.0。

解决方案：在 DHCP 服务器上增加冲突检测次数，避免分配在网络上已存在的 IP 地址。

7) DNS 故障排除

DNS 在 Windows 中起着举足轻重的作用，所以一旦 DNS 服务出现问题可能影响的范围就会很广。DNS 出现问题的现象大多是上不去网，也就是解析不到远程主机的 IP 地址。还有可能就是客户端不能登录域控制器，因为 DNS 无法提供服务。

(1) 服务器“.”问题。

故障原因：很多网络管理员在安装或升级完 Windows 后，经常会发现上不了网，其主要问题就是在安装完 DNS 服务后都会自动把代表根域的“.”加上，导致本地 DNS 服务器不能到网外去查询，客户端也就不会收到希望解析域名的 IP 地址，也就无法访问远程主机。

解决方案：在服务器上删除“.”根域后故障即可解决。

(2) 服务器网关问题。

故障原因：当 DNS 服务器只能提供本地解析服务，而无法提供外部解析服务时，可以查看一下 DNS 服务器的网关是否已经设置，如果没有设置，DNS 无法到外网去作转寄查询，也无法完成客户端提交的外部主机查询请求。

解决方案：在 DNS 服务器上设置正确的网关地址。

(3) DNS 的 SRV 记录。

故障原因：当客户端启动后却无法找到域控制器，检查域控制器一切正常。故障往往都是由 DNS 服务器上的 SRV 记录引起的。

解决方案：确定域服务器已经指向相应的 DNS 服务器，然后在域服务器上找到【管理工具中服务】，在服务中右击 NETLOGON，选择重新启动 NETLOGON 服务，重新注册



SRV 记录。

(4) 客户端指向问题。

故障原因：当客户端无法解析域名时，而 DNS 服务器一切正常，故障通常出在客户端没有正确的配置 DNS 指向。

解决方案：配置合法的 DNS 服务器地址。

(5) 客户端缓存问题。

故障原因：当某台计算机的 IP 地址与主机域名对应关系发生更改时，DNS 服务器已经为其作了更新，而其计算机通过自己的 DNS 名字解析得到的还是以前的 IP 地址，所以无法通信。

解决方案：由于客户端将以前解析过的 DNS 名字放在自己的缓存中，所以需要在客户端上运行 Ipconfig/Flushdns 清除 DNS 缓存，这样就能通过 DNS 服务器重新解析新的 IP 地址。

8) IIS 故障排除

当访问不到网站时，如果检查 DNS 记录没有问题，则故障有可能是在 IIS 服务器上，也有可能是客户端 IE 浏览器的问题。

(1) 服务器站点不稳定问题。

故障原因：如果 DNS 和客户端配置没有问题，那么故障很有可能就是由 IIS 本身的不稳定造成的。Windows 提供的 IIS 5.0 较以前的产品稳定性有了很大的提高，但是如果 IIS 服务器承载的网站过多，或访问量过大时，还是很容易引起不稳定的情况发生。

解决方案：重新启动 IIS，再重新启动访问不到的 Web 站点。

(2) 客户端缓存问题。

故障原因：网站内容已经更新，但是客户端访问的还是旧的内容，那么故障很有可能就是客户端的缓存问题。

解决方案：在客户端的【Internet 选项】|【常规】选项卡中单击删除文件。再选择删除所有脱机内容，单击【确定】按钮清除客户端的缓存。

以上简单介绍了一些比较典型的网络故障现象及其排除方法，具体到每一个不同的网络，其故障现象也会多种多样，总的来说不外乎硬件故障和软件故障两大类。遇到问题时要冷静观察、具体问题具体分析，相信最终能够克服困难，排除故障，让网络重新运转起来。

9.6.4 Windows 局域网使用过程中的常见故障

1. 用户在网络上可以看到其他用户，却无法访问共享资源

故障分析：导致这种故障通常有以下几方面原因，用户的计算机网络连接属性中的文件和打印共享服务没有安装；用户的资源共享设置不正确；网络连接有问题。

解决方法：首先检查用户计算机中的网络连接属性中的文件和打印共享服务是否安装，方法如下。

(1) 双击【控制面板】|【网络连接】图标，在打开的【网络连接】窗口中右击【本地连接】图标，在弹出的快捷菜单中选择【属性】命令，打开【本地连接 属性】对话框，如



图 9.6 所示。



图 9.6 【本地连接 属性】对话框

(2) 在【本地连接 属性】对话框中查看有无【Microsoft 网络的文件和打印机共享】选项，如果没有，说明此项服务没有安装，单击【安装】按钮，在弹出的【选择网络组件类型】对话框中选择【服务】选项，如图 9.7 所示。

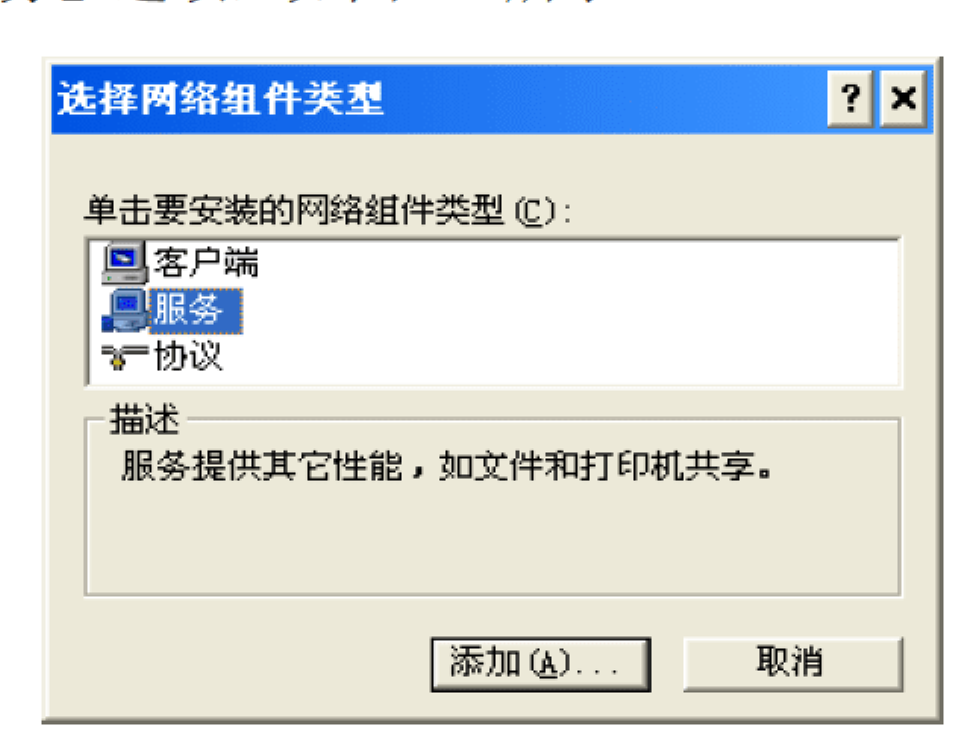


图 9.7 【选择网络组件类型】对话框

(3) 单击【添加】按钮，在打开的【选择网络服务】对话框中选择【Microsoft 网络的文件和打印机共享】选项，然后单击【确定】按钮即可。

(4) 如果 Microsoft 文件和打印机共享服务已经安装好，接下来查看是否所有的协议都绑定了 Microsoft 文件和打印机共享服务，方法是：双击【控制面板】|【网络连接】图标，在打开的【网络连接】对话框中单击【高级】选项卡中的【高级设置】按钮。

(5) 在打开的【高级设置】对话框中查看网络连接，如【本地连接】，如图 9.8 所示，在【高级设置】对话框中【本地连接 的绑定】列表框中，列出了与本地连接绑定的客户端程序、服务以及与客户端程序和服务绑定的各种通信协议，查看这些绑定项目的复选框有没有选中，如果没有选中，请将绑定项目前面的复选框选中。



图 9.8 【高级设置】对话框

最后检查网络连接无问题，可以按照上一小节讲解的方法来检查。

2. 不能共享网络打印机

故障分析：不能共享网络打印机大致有以下几方面原因：网络连接有问题；没有正确安装及设置文件和打印机共享服务；没有正确安装网络打印机驱动程序；网络管理权限的因素。

解决方法：首先检查是否安装了网络打印机的驱动程序，方法是双击桌面上的【网上邻居】图标，在打开的【网上邻居】窗口中，单击左侧的【打印机和传真】选项，然后在打开的【打印机和传真】窗口中检查有没有安装好的网络打印机。 如果没有请安装网络打印机；如果安装好了，还要激活它，将它设置为【默认首选打印机】，方法是右击网络打印机，在弹出的快捷菜单中选择【设为默认打印机】命令即可。

如果打印机驱动程序安装及设置正常，接下来要检查有没有正确安装和配置文件和打印机共享服务。检查和安装方法参见上一故障的排除方法。

如果以上都没有查出问题，还要检查网络连接状况，查看网络打印机是否打开，是否连接在网络上，打印服务器是否打开，工作是否正常，网络连线是否正常。

这些情况都检查后，一般就可以将故障排除。如果故障还是得不到解决，那么还可以检查用户使用网络打印机的权限，比如使用网络打印机的时段、能否访问及使用打印机的用户等情况。因为如果用户在非工作时间或者非使用权限时间使用网络打印机也会造成无法共享网络打印机的“假故障”现象发生。

3. 无法连接到 Internet

故障分析：导致这种故障的原因有以下几个：局域网的问题；代理服务器的问题；Internet 连接的问题。

解决方法：首先检查局域网是否连通，如果局域网没有连通，就根本无法进行 Internet



连接共享。局域网是否连通，主要检查网线、网卡、集线器的连接状况，用户的 TCP/IP 协议配置状况，用户是否登录到域中等。

如果局域网工作正常，各台计算机相互连通正常，接下来检查局域网中的代理服务器是否正确配置、是否工作正常。同时还要检查局域网中的用户身份是否已经被代理服务器正确识别，如果用户身份没有被正确识别，用户也就无法通过代理服务器来共享 Internet。这些主要是通过针对 Active Directory 和 DHCP 服务器的设置加以解决。

如果代理服务器设置无误，工作正常，接下来要检查局域网的 Internet 连接，诸如 Modem、ISDN ADS 等设备的连接状况，如果这些连接出现问题，整个局域网的用户都无法连接到 Internet，一般只需检查是否连接设置方面出了问题。如果是连接设置方面出了问题，请将 Internet 连接进行正确设置。一般经过以上几步检查就可以将故障排除。

4. 在使用过程中网络速度突然变慢

故障分析：以下几个原因可以导致网络速度突然变慢：网络中的设备出现故障；网络通信量突然加大；网络中存在病毒。

解决方法：首先检查是否是因为网络通信量的激增导致了网络阻塞，是否同时有很多用户在传输大量的数据，或者是网络中用户的某些程序在用户发送了大量的广播数据到网络上。对于这种现象，只能尽量避免局域网中的用户同时或长时间地发送和接收大批量的数据，否则就会导致局域网出现阻塞。

如果上述现象没有发生，就要检查网络中是否存在设备故障。设备故障造成局域网速度变慢主要有两种情况：一种是设备不能正常工作，导致访问中断；另一种是设备出现故障后由于得不到响应而不断向网络中发送大量请求数据，从而造成网络阻塞。遇到这种情况，只有及时对故障设备进行维修或者更换，才能彻底解决故障根源。

一般来说，广播风暴通常是由有故障的网卡和集线器造成的，也可能是整个 NetBEUI 网络上过多的广播信息引起的。为了诊断造成广播风暴的故障所在，需要利用协议分析仪来隔离检查这些设备，以便确定故障设备并且更换；如果采用内部路由器和可选路由协议，也可以减弱广播风暴带来的影响，因为路由器并不为广播信息选择路由。

如果网络设备工作正常，那么有可能是病毒造成的网络速度下降。例如，计算机中的蠕虫病毒，受感染的计算机会通过网络发送大量数据，从而导致网络瘫痪。如果网络中存在病毒，请用专门的杀毒软件对网络中的计算机进行彻底杀毒。

9.6.5 故障实例及排除方法

前面介绍了网络故障的种类和原因以及排除网络故障的一般思路和常用工具。本节有针对性地介绍一些网络故障现象的分析和解决方法。

1. 组网过程中的常见故障

在组建局域网过程中，常常会遇到网卡安装不上、网络连接不通等，此时就需要按照前面讲解的排除故障的思路来对故障进行排除。下面简单介绍几种在组网过程中常会遇到的故障现象。

1)　网卡和其他设备冲突，导致不能正常工作

故障分析：在组网过程中经常会遇到安装到系统中的网卡不能正常工作，有时甚至不能启动计算机。这种现象最容易发生在一台安装了两块以上网卡的计算机上，而网卡又最容易和显卡、声卡、内置式调制解调器甚至是和另一块网卡发生资源冲突。当然这种现象也很有可能是由于网卡和主板的插槽没有插牢，导致接触不良从而使得网卡无法正常工作。还有一种可能就是网卡的驱动程序或者网卡坏了。

解决方法：首先将计算机中的其他板卡，如声卡、内置调制解调器等设备拔掉，只保留显卡和网卡，然后重新启动计算机。进入操作系统后，首先安装网卡的驱动程序，然后再安装显卡的驱动程序，如果一切正常则说明网卡和显卡之间的冲突已经解决。一般情况下，先安装网卡驱动后安装其他板卡的驱动就能解决网卡和其他板卡的冲突问题。

如果解决不了，还有一个办法是在 CMOS 中的 PnP/PCI CoMigrations 页面中将 Resources Controlled By 选项的值由 Manual 改为 Auto，同时将系统中不存在设备的设置值改为 Disabled(禁用)，此后重新安装网卡驱动程序，一般都能解决设备冲突问题。

如果以上办法都不行，最后只剩下一种可能情况，那就是网卡的驱动程序不良或者网卡本身有问题，此时建议更换网卡。验证办法就是将此网卡安装到局域网中另一台计算机中查看能否正常工作，如果不能则证明网卡确实有问题，应将其换掉。

2)　网络不通，看不到网上邻居，或者查看网络邻居时提示“无法访问网络”

故障分析：一般出现这种故障现象的原因有以下几种情况，网线不良或者没有插好；网卡安装不正确；网络属性没有设置好。

操作步骤如下。

(1)　首先检查网线是否良好，接头是否安插到位。先检查网线的接触状况。网线的接触状况主要指网线和计算机网卡的接触情况，以及网线和集线器接口的接触状况。

①　先检查网线和计算机网卡的接触情况，然后检查网线和集线器接口的接触状况。

②　如果接插部位接触良好，将网线拆下来检查网线的类型对不对，如果是双机跳接线，请将其更换为直连线。

(2)　接下来具体检查网线的物理状况。网线是由一根线和两个水晶头组成的，网线的问题主要集中在水晶头上，可按以下顺序进行检查。首先，检查水晶头的弹性。好的水晶头的防松卡(Loosepreventer) 弹性非常好，插入网卡插座时，能听到清脆的“咔嗒”声。质量差的水晶头，其防松卡插进插座时声音很小或没有声音，插拔几次就失去弹性，插头与插座的间隙越来越大，接触性能变差，稍一受力就会出现网络时通时断的现象。其次，检查水晶头的压线片。网线是靠压线片与插座内的弹性金属丝的接触连通网卡的。使用时间较长或质量较差的水晶头压线片会松弛，从水晶头上脱落，从而造成网络不通。另外，制作网线时，由于制作粗心或水晶头质量太差，有时网线绝缘皮未能压在水晶头内。这种网线开始使用时一般不会出现问题，但时间长了，网线受力后可能会从水晶头内脱落造成网络不通。最后，检查网线通路，可以用电缆测试仪测试其连通状况，如果网线不良将其换掉，如果网线正常，就排除了网线方面的因素。

(3)　随后，进入操作系统检查网卡的安装状况。在此以 Windows XP 为例加以介绍(风格为经典设置)。在桌面上右击【我的电脑】图标，在弹出的快捷菜单中选择【属性】命令，打开【系统属性】对话框，在【硬件】选项卡中单击【设备管理器】按钮，打开【设备管



理器】窗口，如图 9.9 所示。在其中检查【网络适配器】选项前面是否有黄色的惊叹号，如果有叹号，则说明该设备没有安装好，如果没有叹号则说明该设备安装正确。

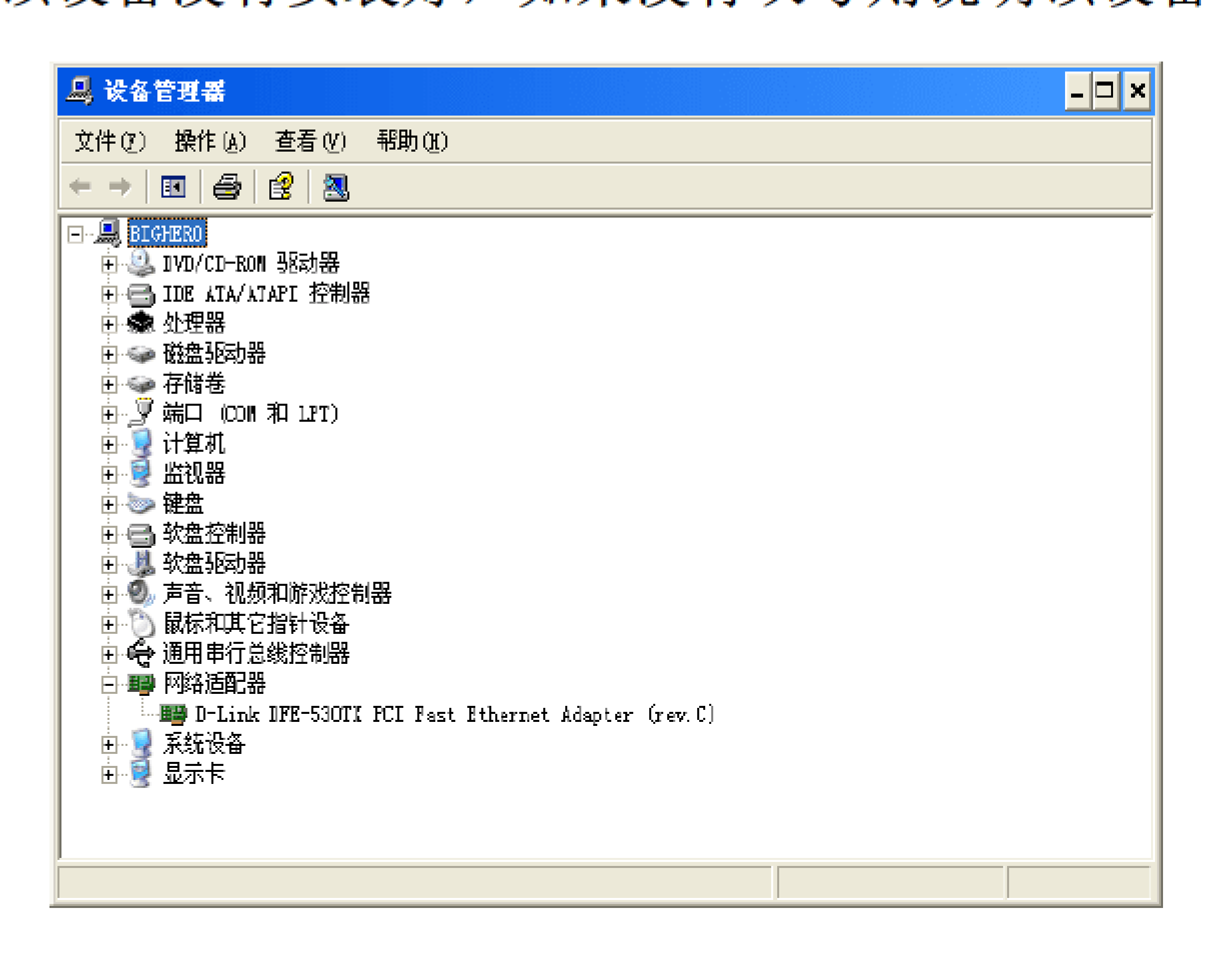


图 9.9　检查【网络适配器】选项前面是否有黄色的惊叹号

如果网卡安装正确，接下来检查网络属性的设置情况，一般在局域网中需要给每台计算机一个确定的且各不相同的网络 IP 地址和网络标识；否则会导致看不到网上邻居。具体检查步骤如下。

① 先检查网络标识。在桌面上右击【我的电脑】图标，在弹出的快捷菜单中选择【属性】命令，打开【系统属性】对话框，切换到【计算机名】选项卡，如图 9.10 所示。

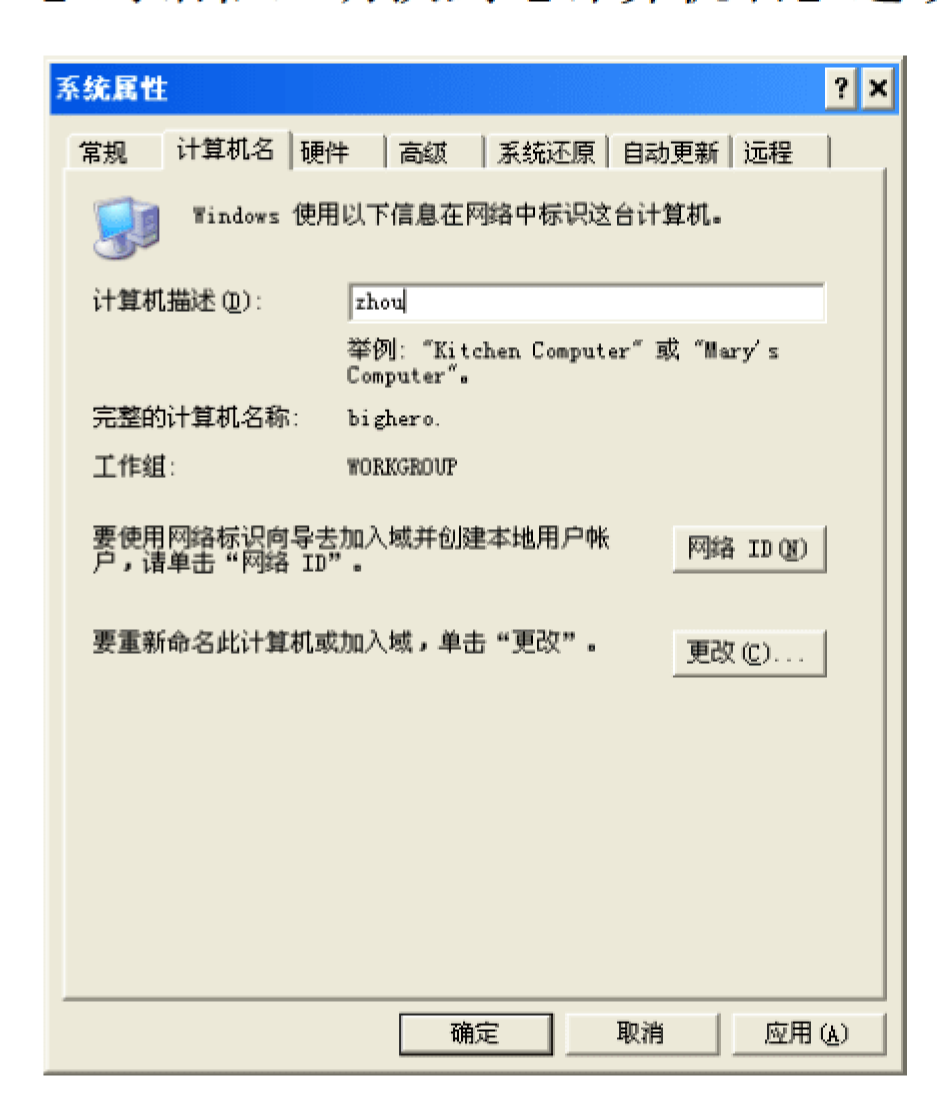


图 9.10　【计算机名】选项卡

② 在【计算机名】选项卡中单击【更改】按钮，打开【计算机名称更改】对话框，如图 9.11 所示。在该对话框中查看计算机的网络标识，如果指定的【域】或者【工作组】名称正确，则完成确认工作。

③ 接下来检查网络 IP 地址的设置状况，在桌面上右击【网上邻居】图标，在弹出的快捷菜单中选择【属性】命令，打开【网络连接】窗口，右击【本地连接】选项，在弹出的快捷菜单上选择【属性】命令，打开【本地连接 属性】对话框，如图 9.12 所示。

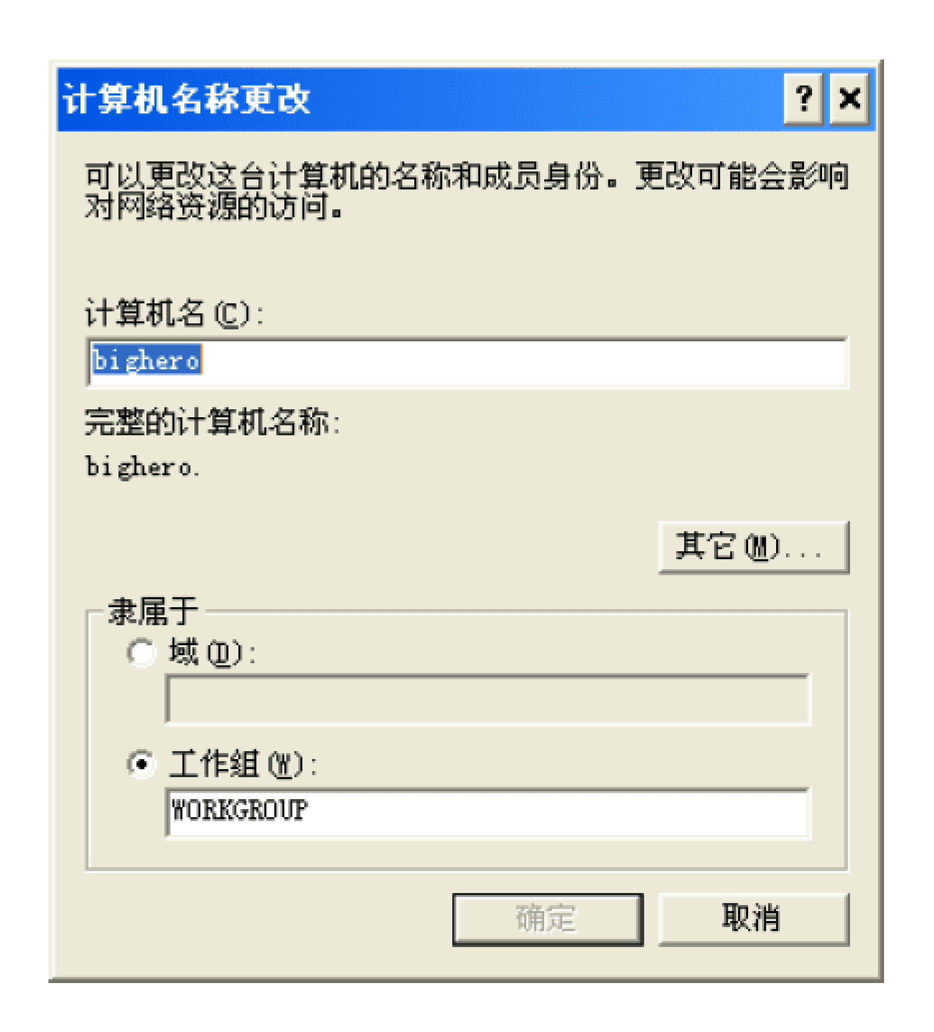


图 9.11　【计算机名称更改】对话框

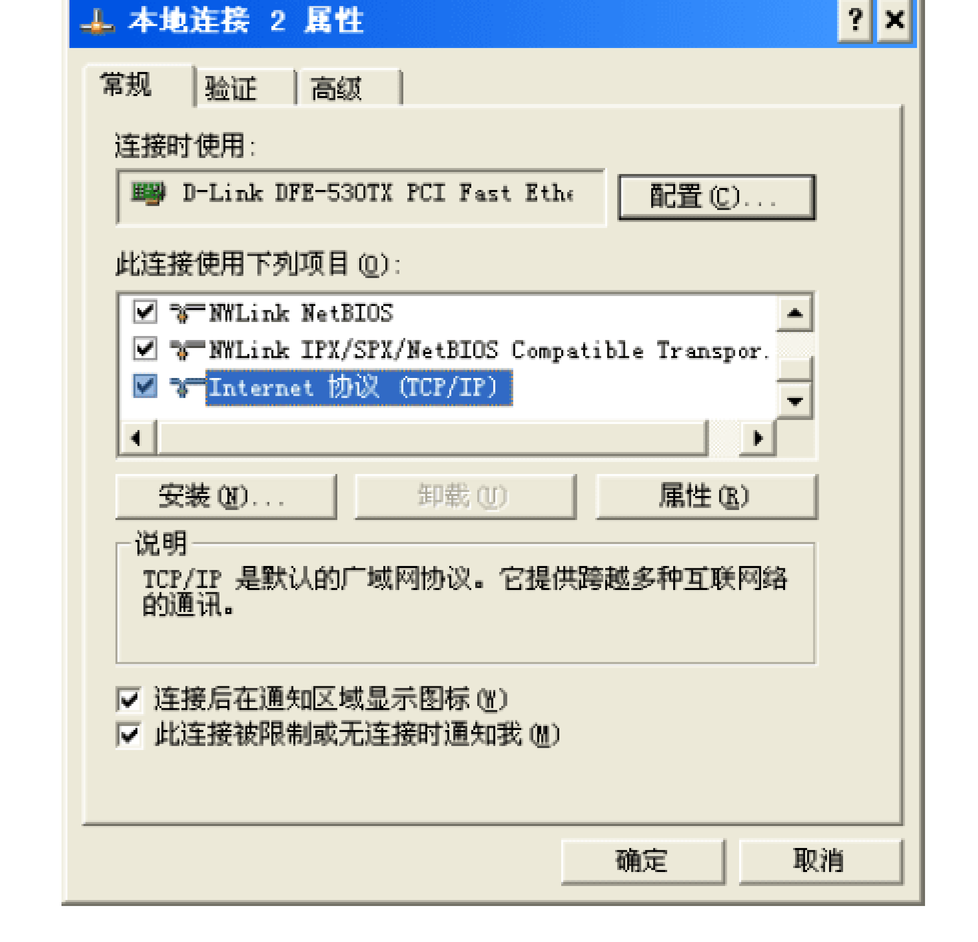


图 9.12　【本地连接 属性】对话框

④　在该对话框中选择【Internet 协议(TCP/IP)】选项，然后单击【属性】按钮，打开【Internet 协议(TCP/IP)属性】对话框，如图 9.13 所示。在其中确认网络 IP 地址是否被正确设置，如果没有请将其正确设置。经过以上检查步骤，故障一般都能排除。

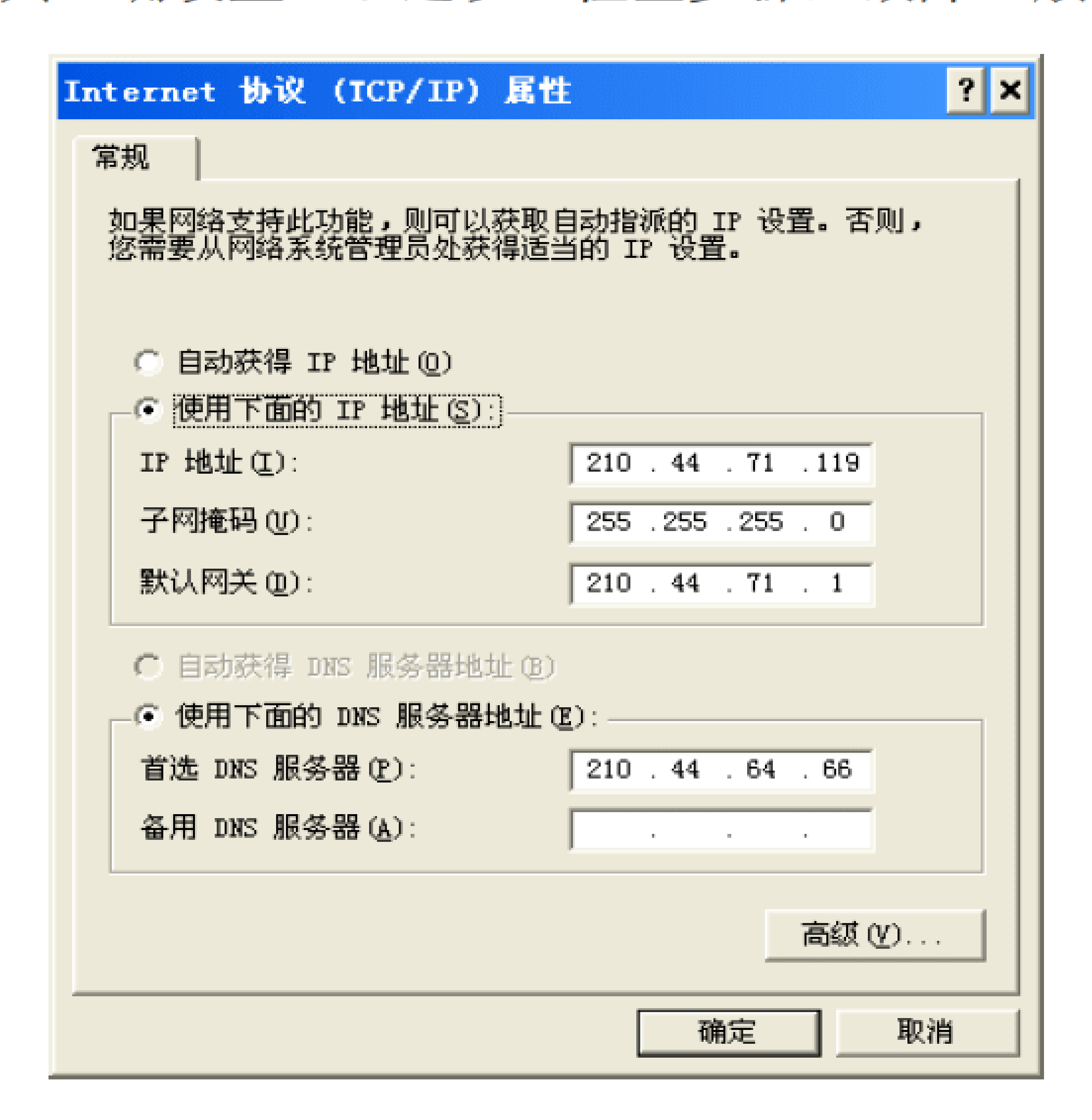


图 9.13　【Internet 协议(TCP/IP)属性】对话框

3)　用户无法登录到 Windows 域中

故障分析：这种现象一般在新手组建局域网时经常出现，造成这种故障现象的原因有多种。例如，用户在服务器中没有创建相应客户机的登录账户和密码；客户机没有加入到域环境中来；网络连接不正常；服务器工作状况不良等。

解决方法：一般情况下，在局域网中创建了域服务器后一般都会给客户机创建相应的登录账户，也会将客户机一端加入到域环境中，所以出现此类故障时，前两种原因的可能性比较小，除非有人将客户机一端从【域】改动到【工作组】，或者将客户机的登录账号删除了，否则不会由于前两种原因导致此故障的发生。但是为了保险起见，最好检查一番服务器和客户机的设置情况。



首先，检查网络的连接状况，查看网络连接是否正常。网络连接中最常见的问题是网线和集线器的连接状况，重点检查域控制器的网线和客户机的网线是否松动。

接下来检查服务器的工作状况。一般情况下，服务器出问题的概率不大，但是如果服务器出现故障，用户将无法登录到 Windows 域中，所以要检查服务器是否关机、死机，是否有重要服务项目出错。可以使用【事件查看器】来检查服务器工作状态。通过查看事件日志，系统管理员可以很方便地得知系统出现的问题及可能的原因。要查看事件日志需要先打开【事件查看器】窗口。首先在【控制面板】窗口中双击【管理工具】图标，打开【管理工具】窗口，然后在打开的【管理工具】窗口中双击【事件查看器】图标，即可打开【事件查看器】窗口，如图 9.14 所示。有关事件查看器的具体使用请参阅【帮助】菜单。

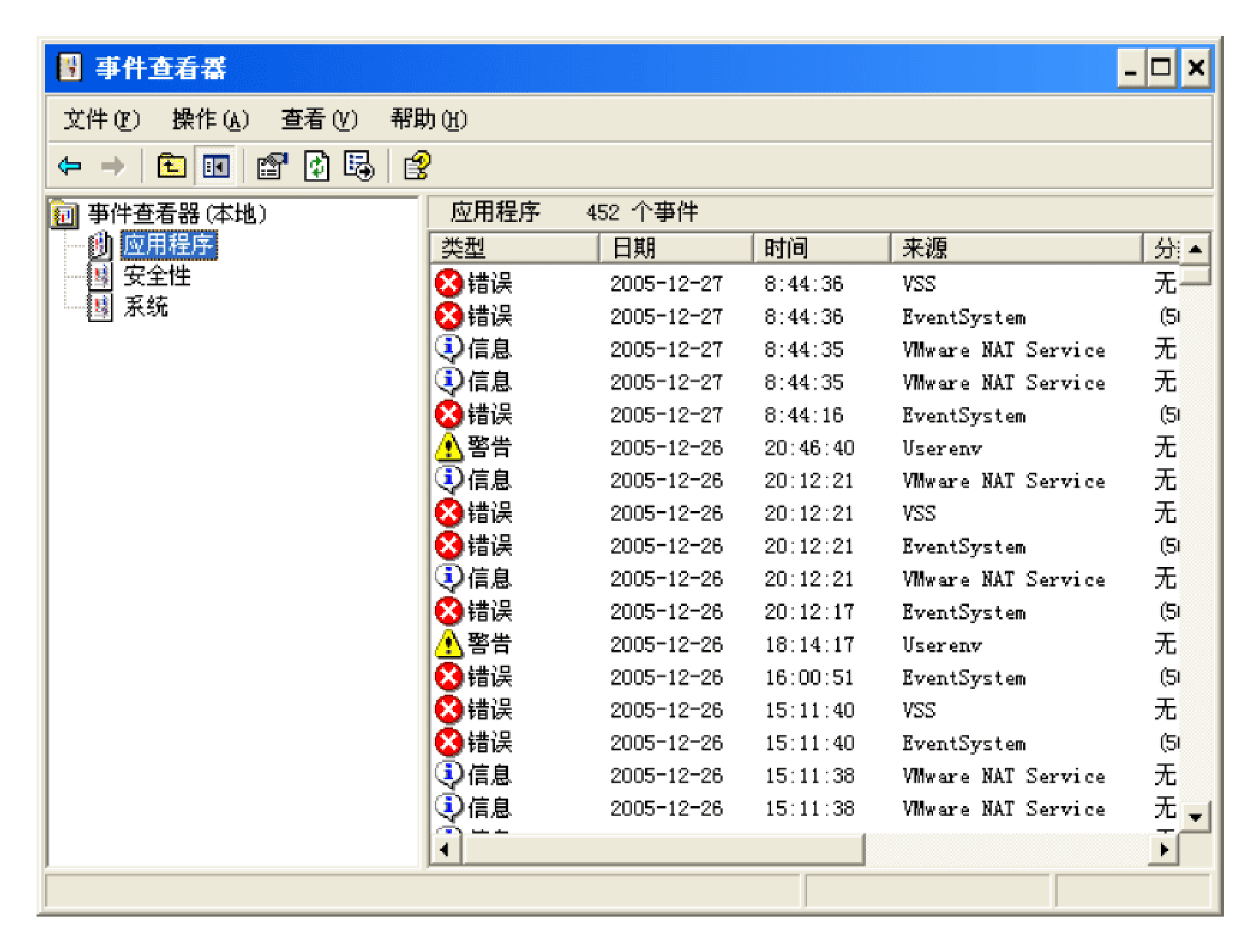


图 9.14 【事件查看器】窗口

如果发现服务器端工作良好，接下来检查服务器上用户账号、密码是否正常，客户机的账号是否被锁定。如果都正常，接下来检查客户机的 TCP/IP 设置状况，具体方法是使用 Ipconfig 命令检查客户机端是否正确设置了要登录的域，是否安装了需要的网络组件等。一般经过这番检查都能将故障排除。

4) 登录时 IP 地址冲突现象

故障分析：此类故障大都是由于手动为局域网中的用户分配 IP 地址资源时发生重复而导致。

解决方法：有两种方法可以解决这个问题。一种是将局域网中的 IP 地址重新进行规划，为所有的资源分配 IP 地址。但是这种方法的缺点是静态划分 IP 地址，不能适应局域网中资源的动态变化，如果局域网中增加设备时还会引发冲突。另一种解决方法是动态划分 IP 地址。在域控制器上架设 DHCP(动态主机配置协议)。DHCP 服务器为局域网中的各种设备动态地分配 IP 地址，并对已经分配的地址进行保留，有效地避免了资源冲突。

复习思考题九

一、填空题

1. 网络管理结构中的被管设备又被称为网络元素，是指________________。

2. SNMP 标准主要由 3 部分组成：____。

3. SNMP v3 主要定义了 SNMPv2 里缺少的网络安全方面的____________、____________、____________。以上 3 种功能所需的远程配置和管理能力 4 个关键域。

4. 紧急响应的主要阶段包括__________、__________、__________、根除阶段、恢复阶段、报告和总结阶段等。

5. 防范网络监听可以采取的措施有从逻辑或物理上对网络分段、以交换式集线器代替共享式集线器、__________、__________。

6. 按数据备份时备份的数据不同，可有__________、__________、__________和按需备份等备份方式。

7. __________是指在多用户的环境下，对数据库的并行操作进行规范的机制，从而保证数据的正确性与一致性。

二、选择题

1. 按数据备份时数据库状态的不同有(　　)。
   A. 热备份　　B. 冷备份　　C. 逻辑备份　　D. A、B、C 都对
2. 端口扫描是一种(　　)型网络攻击。
   A. DoS　　B. 利用　　C. 信息收集　　D. 虚假信息
3. (　　)不是 Internet 服务的安全隐患。
   A. E-mail 缺陷　　B. FTP 缺陷　　C. USENET 缺陷　　D. 操作系统缺陷
4. (　　)攻击是一种特殊形式的拒绝服务攻击，它采用一种分布、协作的大规模攻击方式。
   A. DDoS　　B. DoS　　C. 缓冲区溢出　　D. IP 电子欺骗

三、判断题

1. 网络管理就是为保证网络系统能够持续、稳定、安全、可靠和高效地运行、不受外界干扰，对网络系统设施采取的一系列方法和措施。(　　)
2. 网络计费管理从网上收取费用。(　　)
3. 网络资源管理指的是与网络有关的设备。(　　)
4. 网关是连接两个不同类型的局域网络的网络连接设备。(　　)
5. 封装性是将对象包含的特殊化信息和操作隐藏在对象内部，对外提供标准属性和操作。(　　)
6. ODBC 为用户提供了一个简单、标准和透明的数据库连接的公共编程接口，各开发



厂商根据 ODBC 的标准来实现其底层的驱动程序。 ( )

7. 增量备份指每次备份的数据是相对于上一次备份后增加的数据。 ( )

8. 容错是为了防止网络系统内部的某些子系统出现故障，而容灾是为了防止由于自然灾害等导致的整个系统全部或大部分受到损坏。 ( )

四、简答题

1. 什么是路由器?它有哪些功能?
2. 请说明 MAC 地址查找方式中动态主机配置协议(DHCP)的基本步骤。
3. 什么是网络通信协议？它有哪些特点？
4. 要查找 w.x.abc.com 的 IP 地址，请写域名解析的具体步骤。
5. Windows 自带网络工具箱常用命令的功能是什么？
6. 局域网常见故障排除思路是什么？
7. 上网常见故障的排除方法有哪些？
8. 交换机的 MAC 地址列表有问题用什么方法解决？
9. 网线的种类及连接方法。
10. IP 地址配置有问题用什么方法解决？
11. DHCP 有故障用什么方法解决？
12. DNS 有故障用什么方法解决？

第 10 章　网络信息安全系统设计案例

学习目标

学习网络信息安全系统设计的总体目标方案需求，涉及需求分析、工程论证、网络安全总体目标、设计原则以及具体的网络安全方案等几个方面。通过本章的学习，读者应掌握及了解以下内容。

- 掌握网络信息安全系统设计的需求分析、工程论证、总体目标、设计原则以及具体设计等问题。
- 了解现代企业的网络安全实体设计问题。

10.1　确定企业网络设计目标

网络安全是所有网络用户都普遍关心的问题，一旦 PC 与网络连接，就面临着网络安全问题。引起网络安全的直接原因，就是网络系统的安全漏洞。现在的网络安全的开发，大部分都是走补堵安全漏洞的道路。随着网络系统的日益复杂，网络的安全漏洞会层出不穷，这种思路下的安全防护，将永远跟着“黑客”走。所以，随着网络安全技术的发展，应该走系统集成的道路，也就是多重安全措施并存，这实际上就是网络信息安全系统。

10.1.1　需求分析

网络的需求分析是关系到一个网络系统成败的关键，是网络设计的基础，必须把网络应用的需求分析作为网络系统规划与设计中至关重要的步骤来认真完成，了解用户建网的目的、用户已有的网络基础和应用现状(包括综合布线、网络平台、已开展的网络应用等)。

需求分析最终应得出对网络系统的以下几个方面的明确定义：网络的地理分布；确定网络覆盖的地理范围，以及网络节点的数量和位置、站点间最大的距离、用户群组织、特殊要求和限制；用户设备类型；网络带宽和网络服务质量；网络安全和网络管理系统的需求。

明确网络安全的系统需求，明确网络管理范围、网络管理对象和用户对网络管理功能的需求。网络管理功能涉及网络配置管理、性能管理、故障管理、安全管理和计费管理等 5 个方面。

需求分析是组建网络的基础，除了应明确上述几个方面的定义外，还要考虑机房的环境(温度、湿度及抗干扰性等)和位置需求、网络设备的电气特性(电源、接地、防雷击等)、网络管理和应用人员的状况、用户未来发展的需求等诸多方面。

10.1.2　工程论证

工程论证是为了弄清所定义的项目是否可能实现和是否值得进行研究，论证的过程实



际是一次大大简化了的系统分析和系统设计的过程。在投入大量资金前研究工程的可能性，减少所冒的风险，即使研究结论不值得进行，花在可行性研究上的精力也不算白费，因为它避免了一次更大的浪费。

在论证过程中需要从经济、技术、运行和法律等诸多方面进行论证，得出明确的结论供用户参考。在经济方面，需要论证局域网的设计有没有经济效益、花费如何、多长时间可以收回成本。在技术方面，包括现有技术如何实现这一方案、有没有技术难点、建议采用的技术先进程度怎样、系统有无可扩展性、可满足未来多少年内的增长需求、系统是否有冗余、所提供的稳定性能否满足用户要求。运行可行性指工程的运行方式是否可行，工程中有无一定的安全措施可以保证网络的正常运行，系统中有无安全漏洞。法律可行性指工程的实施会不会在社会上或政治上引起侵权、破坏或其他责任问题等。

10.2　现代企业网络安全总体设计思想

10.2.1　现代企业网络安全方案的总体目标

(1)　建设开放复杂系统所需的相对完整、实用的安全技术体系。

(2)　结合当前最新技术和产品，定义安全防御体系实现框架。

(3)　以信息安全工程建设和信息安全服务的规范为指导，提供完备的安全工程实施和解决方案。

(4)　建设与系统规模和性质相适应的 24h 紧急事件响应和维修体系。

(5)　企业各部门信息能够及时、准确地传输到集团公司决策部门和管理部门。

(6)　异地分支机构能够与企业总部中心网络互联起来，以便下载、上传业务数据，以及使用电子邮件。各部门、分支机构可以相互独立，互不干扰。

(7)　网管中心提供统一的外部互联接口，能够保证集团公司企业内部网的信息安全，提供集团公司内部的信息服务。

(8)　企业有扩展的需要，要预留接口。

10.2.2　现代企业网络安全设计原则

在对这个企业局域网网络系统安全方案设计、规划时，应遵循以下原则。

1. 综合性、整体性原则

应用系统工程的观点、方法，分析网络的安全及具体措施。安全措施主要包括行政法律手段、各种管理制度(人员审查、工作流程、维护保障制度等)及专业措施(识别技术、存取控制、密码、低辐射、容错、防病毒、采用高安全产品等)。一个较好的安全措施往往是多种方法适当综合的应用结果。一个计算机网络，包括个人、设备、软件、数据等。这些环节在网络中的地位和影响作用，也只有从系统综合整体的角度去看待、分析才能取得有效、可行的措施。即计算机网络安全应遵循整体安全性原则，根据规定的安全策略制定出合理的网络安全体系结构。



2. 需求、风险、代价平衡的原则

对任一网络，绝对安全难以实现，也不一定是必要的。对一个网络进行实际研究(包括任务、性能、结构、可靠性、可维护性等)，并对网络面临的威胁及可能承担的风险进行定性与定量相结合的分析，然后制定规范和措施，确定本系统的安全策略。

3. 一致性原则

一致性原则主要是指网络安全问题应与整个网络的工作周期(或生命周期)同时存在，制定的安全体系结构必须与网络的安全需求相一致。安全的网络系统设计(包括初步或详细设计)及实施计划、网络验证、验收、运行等都要有安全的内容及措施，实际上在网络建设的开始就考虑网络安全对策，比在网络建设好后再考虑安全措施不仅容易而且花费也小得多。

4. 易操作性原则

安全措施需要人为去完成，如果措施过于复杂，对人的要求过高，其本身就降低了安全性。其次，措施的采用不能影响系统的正常运行。

5. 分步实施原则

由于网络系统及其应用扩展范围广阔，随着网络规模的扩大及应用的增加，网络脆弱性也会不断增加，一劳永逸地解决网络安全问题是不现实的；同时由于实施信息安全措施需相当大的费用支出，因此分步实施，即可满足网络系统及信息安全的基本需求，亦可节省费用开支。

6. 多重保护原则

任何安全措施都不是绝对安全的，都可能被攻破。但是建立一个多重保护系统，各层保护相互补充，当一层保护被攻破时，其他层仍可保护信息的安全。

7. 可评价性原则

如何预先评价一个安全设计并验证其网络的安全性，这需要通过国家有关网络信息安全测评认证机构的评估来实现。

10.3　现代企业网络安全的整体设计需求

10.3.1　物理安全设计

保证计算机信息系统各种设备的物理安全是保障整个网络系统安全的前提。物理安全是保护计算机网络设备、设施以及其他媒体免遭地震、水灾、火灾等环境事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏过程。它主要包括以下 3 个方面。

(1)　环境安全。对系统所在环境的安全保护，如区域保护和灾难保护等。

(2)　设备安全。设备安全主要包括：设备的防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等；设备冗余备份；严格管理及提高员工的整体安全意识来实现。



(3) 媒体安全。其包括媒体数据的安全及媒体本身的安全。显然，为保证信息网络系统的物理安全，除在网络规划、场地、环境等要求外，还要防止系统信息在空间的扩散。计算机系统通过电磁辐射使信息被截获而失密的案例已经很多，在理论和技术支持下的验证工作也证实这种截取距离在几百甚至可达千米的复原显示技术给计算机系统信息的保密工作带来了极大的危害。为了防止系统中的信息在空间的扩散，通常是在物理上采取一定的防护措施，来减少或干扰扩散出去的空间信号。

10.3.2 边界保护设计

1. 物理隔离的方案

对于企业外网和科研内网独立布线，物理线路上实现隔离。对上外网的计算机，采用专机和物理隔离卡相结合的方式，研究部和其他人员较多的部门选用专机上网，领导和人数较少的部门使用物理隔离卡的方式上外网。实现物理隔离具有以下优势。

(1) 内外网绝对隔离。将单一的 PC 从物理上分隔成两个虚拟工作站，它们分别有自己独立的硬盘和操作系统，并能通过各自的专用接口与网络连接，从而最大限度地保证了安全(内网)与非安全(外网)环境的物理隔离。

(2) 完全控制。安全策略的实施安装在主板和两块硬盘之间，完全控制硬盘通道，并通过继电器来控制内网和外网间的硬盘转换和网络连接，保证其工作状态的稳定性及可靠性。

(3) 转换自如。用户可根据需要在任何时间、任何系统中方便、自如地进行内部网和外部网之间的转换。

(4) 两种切换方式。硬切(按钮切换)和软切(软件切换)均可实施。

(5) 应用广泛。不依赖于操作系统，可以应用于所有使用 IDE-ATA 硬盘的 PC 系统，可以适用于局域网、宽带等不同的网络环境。

(6) 对网络技术、协议完全透明；安装方便，操作简单，不需要用户进行专门的维护。

2. 以防火墙密码技术为基础的网络强隔离系统

网络强隔离系统是由外部访问控制服务器、安全隔离与信息交换设备和内部访问控制服务器组成的具有层次结构的系统。网络强隔离系统是保卫外部边界的有力措施，对流入、流出边界的数据流进行有效的控制和监督，如图 10.1 所示。



图 10.1 网络强隔离系统

防火墙的使用是非常灵活的，可以在以太网的任意部位进行链路分割，构成安全的网络范围。可以用于在单位内网同外界的广域网出口上，实现对单位内网的保护；可以在内部网络上进行划分，建立局部的安全区；可以单独设置在某一台或几台重要的服务器对这



些服务器进行安全保护。

企业网络由多个具有不同安全信任度的网络部分构成，在控制不可信连接、分辨非法访问、辨别身份伪装等方面存在着很大的缺陷，从而构成了对网络安全的重要隐患。设计中，采用防火墙设备确保如财务部、开发部等重要安全域的相对独立。选购防火墙主要应从安全角度考虑，在这里效率不应成为瓶颈问题，应该选购业界大公司或资深信息安全研制单位的成熟产品以满足系统安全的需要。

通过在核心交换机和高性能服务器群之间及核心交换机和重要部门之间部署防火墙，通过防火墙将网络内部不同部门的网络或关键服务器划分为不同的网段，彼此隔离。这样不仅保护了该单位网络服务器，使其不受来自内部的攻击，也保护了各部门网络和数据服务器不受来自该单位内部其他部门的网络攻击。如果有人擅自闯进一个部门，或者如果病毒开始蔓延，网段能够限制造成的损坏进一步扩大。

防火墙根据系统管理者设定的安全规则保护内部网络，提供完善的安全性设置，通过高性能的网络核心节点进行访问控制。同时提供网络地址转换、透明的代理服务、信息过滤、内容过滤、双机热备份、流量控制、带宽管理及用户身份认证等功能。

3. 网络安全检测

利用防火墙并经过严格配置，可以阻止各种不安全访问通过防火墙，从而降低安全风险。但是，网络安全不可能完全依靠防火墙单一产品来实现，网络安全是一个整体，必须配置相应的安全产品，作为防火墙的必要补充。网络系统的安全性取决于网络系统中最薄弱的环节，如何及时发现网络系统中最薄弱的环节，如何最大限度地保证网络系统的安全，最有效的方法是定期对网络系统进行安全性分析，及时发现并修正存在的弱点和漏洞。

网络安全检测工具通常是一个网络安全性评估分析软件，其功能是用实践的方法扫描分析网络系统，检查报告系统存在的弱点和漏洞，建议采取的补救措施和安全策略，以达到增强网络安全的目的。

入侵检测系统是根据已有的、最新的攻击手段的信息代码对进出网段的所有操作行为进行实时监控、记录，并按制定的策略实行响应(阻断、报警)，从而防止对网络的攻击与犯罪行为。入侵检测系统一般包括控制台和探测器(网络引擎)。控制台用作制定及管理所有探测器(网络引擎)。探测器(网络引擎)用作监听进出网络的访问行为，根据控制台的指令执行相应行为。由于探测器采用的是监听而不是过滤数据包，因此，入侵检测系统的应用就不会对网络系统的性能造成多大影响。

10.3.3　网络系统安全设计

网络系统安全包括网络操作系统及网络应用系统的安全两个方面。

1. 网络操作系统安全

对于网络操作系统的安全防范可以采取以下策略：尽量采用安全性较高的网络操作系统，并进行必要的安全配置，关闭一些并不常用却存在安全隐患的应用、服务及端口。对一些保存有用户信息及其口令的关键文件使用权限进行严格限制；加强口令字的使用(增加口令复杂程度、不要使用与用户身份相关的、容易猜测的信息作为口令，要经常更换口令)



并及时给系统打补丁、系统内部的相互调用不对外公开。

2. 网络应用系统安全

在应用系统安全上，应用服务器尽量不要开放一些没有经常用的协议及协议端口号(如文件服务、电子邮件服务器等应用系统)，可以关闭服务器上的如 HTTP、FTP、Telnet 等服务。加强登录身份认证，确保用户使用的合法性，严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。充分利用操作系统和应用系统本身的日志功能，对用户所访问的信息做记录，为事后审查提供依据。同时还要及时升级各种已经发布的升级补丁程序，以减少因为升级过程周期长而带来攻击事件的发生。

10.3.4 建立有效的信任体系

1. 证书管理系统

采用基于国际标准的 PKI 技术体系开发的证书和密钥管理系统，它由五大子系统组成，即证书注册子系统、证书签发子系统、证书发布和查询子系统、密钥管理子系统和备份子系统。证书管理系统具有符合标准、开放、安全性高、功能全面、工作流程简单清晰、配置灵活等特点，并提供了与其他 PKI/CA 体系的接口，易于扩展。可以作为大型的 CA 中心系统，也可以作为企业级的 CA 中心系统。

2. 目录服务器

目录服务器是方案的基石，目录服务器集中存储用户身份信息、服务数据、访问策略和证书等，对用户可信性的鉴别过程高度依赖于可信数据存储的性能。目录系统成功实施的关键在于建立高扩展性、高可靠性的目录服务器集群，应用程序用它们进行认证。

目录服务器是整个应用层面访问控制的基础，是统一用户管理的核心，所以目录服务器的高可用性是非常重要的。系统中包含 4 个目录服务器，其中内部两个为主目录服务器，包含了所有相关记录，两个目录服务器相互复制来保证它们总是含有最新数据，这样任何一个服务器的失败都不会造成信息的损失。外网所需要的客户信息，电子商务应用所需要的客户信息将被复制到外部目录服务器上，提供客户认证服务，对于企业的一些经常需要跨网操作的用户来说，他们的信息将被复制到所有地域性的目录服务器上，这样可以在每个区域网内为他们进行有效的认证授权服务。

3. 认证服务器

认证服务器用于对内、外部网络的 Web 方式和非 Web 方式应用进行访问认证和授权控制，并且保证提供的这种访问控制服务的稳定性，这样可以保证商业信息的安全传输。另外，用户只需要提交一次认证信息就可以访问相应资源的单点登录方式，极大地提高了用户使用的方便性。

认证服务器的主要功能是认证服务和授权策略管理。用户认证/授权管理平台实现了统一的用户身份管理的功能，即实现了一致性的安全策略、集中管理的认证和授权机制、完整的身份活动周期管理。实现统一的用户身份管理的优点有以下几点。

(1) 增强安全性。集中式的策略管理，实现单点访问控制；通过数字证书、令牌卡、

智能卡等手段增强应用程序和资源的安全性。

(2)　方便经济。单点登录方便使用、提高用户效率；集中式的用户、策略和服务管理减少维护工作量。

(3)　提高运行效率。对各种服务而言，在身份认证服务器上即可实现创建、维护和删除用户账号等各种功能；在各种数据源之间保持信息同步，如 Windows 账号、邮件账号和人力资源系统等。

4. 单点登录系统

单点登录(Single Sign On，SSO)就是合法用户一次登录就可以访问多个应用程序。单点登录使用户可以基于最初访问应用时的一次身份认证，对所有被授权的应用进行无缝的访问，不需要用户多次输入用户名和口令，减少了用户的等待时间，提高用户工作效率。实现 SSO 方案的原理是共享一个身份认证标识(SSO Token)，当用户使用 Identity Server 支持的认证机制(如证书)向 Identity Server 请求认证时，将产生身份认证标识 SSO Token，SSO Token 将发送回客户端。当用户再访问其他应用时，只要出示这个身份认证标识 SSO Token，如果此身份认证标识 SSO Token 合法，则不需要用户再进行身份认证。

10.3.5　病毒防护

未来的网络威胁将以传播病毒的速度越来越快、发现漏洞到利用漏洞进行攻击时间越来越短为特征。为此，无论是手动的还是自动的应对措施都将不起作用，唯一的方法是主动预防，即部署整体的网络安全解决方案，而不是简单的反病毒解决方案。原来通常在自己的 PC 上安装防毒软件来保护系统，对于单节点而言，只要能够确保防毒软件有效，能及时更新病毒特征码，就可以防范绝大多数的病毒，如果还想防范结合 Hacker Overflow 技术的病毒，还需要及时给操作系统打补丁。显然，这些操作需要相当高的计算机操作水平，但是这种方式在一个企业的网络环境中通常不能达到令人满意的效果，原因有以下几点。

首先，企业的网络通常有成百上千的主机，很难保证所有节点(包括移动节点)的防毒系统都处在最佳的状态，包括是否安装防毒软件、防毒系统是否生效、是否更新到了最新的病毒特征码、是否给操作系统打好了最新的安全补丁等许多影响终端节点防毒的因素。其次，网络病毒的传播和防毒系统的特征码更新都是利用网络，它们之间只是时间上的对抗，由于病毒的出现肯定要先于病毒特征码的出现，从而在客观上造成拥有大量终端节点的企业防病毒体系在与网络病毒的对抗中处在一个不利的境地。

要想在这场对抗中获得主动，眼光自然移到了企业的网络边缘上，在网络入口挡住有害数据。在本书的方案中，采用“扫进又扫出”的病毒扫描和内容过滤策略，不仅对进入企业内部网的请求进行病毒扫描和内容过滤，而且还在内部用户访问 Internet、内部广域网之前，在本地网络边界进行病毒扫描和内容过滤，从而防止了用户的关键业务受到病毒、恶意代码的破坏，提高了用户网络的安全性和可用性。

10.3.6　数据备份恢复

为了保护重点服务器的完整性，防止其上的信息被非法篡改，保护系统运行安全，应使用服务器灾难恢复系统。服务器灾难恢复系统可以将服务器上的重要信息进行备份，并



定期检测服务器上信息内容的完整性，一旦发现信息被非法篡改，就会使用原始数据对服务器进行灾难恢复。该系统适合于计算机网络中对外发布信息的服务器和内部重要的服务器群，也可以用于其他基于文件系统的服务器，如 FTP、E-mail 和 DNS 服务器等。

同时制定完善的安全备份管理制度，如系统安全备份规范、数据介质保存规定等；数据备份则主要通过磁盘、磁带、光盘等介质来进行。

备份系统为一个目的而存在，这就是尽可能快地全盘恢复运行计算机系统所需的数据和系统信息。根据系统安全需求可选择的备份机制有：场点内高速度、大容量自动的数据存储、备份与恢复；场点外的数据存储、备份与恢复；对系统设备的备份。备份不仅在网络系统硬件故障或人为失误时起到保护作用，也在入侵者非授权访问或对网络攻击及破坏数据完整性时起到保护作用，同时也是系统灾难恢复的前提之一。

在确定备份的指导思想和备份方案后，就要选择安全的存储介质和技术进行数据备份，有“冷备份”和“热备份”两种。热备份是指“在线”的备份，即下载备份的数据还在整个计算机系统和网络中，只不过传到另一个非工作的分区或是另一个非实时处理的业务系统中存放。“冷备份”是指“不在线”的备份，下载的备份存放到安全的存储介质中，而这种存储介质与正在运行的整个计算机系统和网络没有直接联系，在系统恢复时重新安装，有一部分原始的数据长期保存并作为查询使用。

热备份的具体做法是可以在主机系统开辟一个非工作运行空间，专门存放备份数据，即分区备份；另一种方法是，将数据备份到另一个子系统中，通过主机系统与子系统之间的传输，同样具有速度快和调用方便的特点，但投资比较昂贵。冷备份弥补了热备份的一些不足，二者优势互补、相辅相成，因为冷备份在回避风险中还具有便于保管的特殊优点。

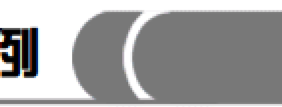
10.3.7 安全管理制度

制定安全管理策略和原则，如用户授权实施细则、口令字及账户管理规范、权限管理制度等。同时还要建立健全安全管理机构：为保证各部门计算机网络系统正常、有效和安全地运行，必须首先建立健全一套与之相应的政府部门计算机网络安全管理机构。

10.4 现代企业的网络信息安全风险分析

随着 Internet 网络急剧扩大和上网用户迅速增加，风险变得更加严重和复杂。原来由单个计算机安全事故引起的损害可能传播到其他系统，引起大范围的瘫痪和损失。再加上缺乏安全控制机制和对 Internet 安全政策的认识不足，这些风险正日益严重。

针对现代企业局域网中存在的安全隐患，在进行安全方案设计时，下述安全风险必须要认真考虑，并且要针对面临的风险，采取相应的安全措施。这些风险由多种因素引起，与现代企业局域网结构和系统的应用、局域网内网络服务器的可靠性等因素密切相关。网络安全可以从以下几个方面来理解：物理网络是否安全；网络平台是否安全；网络系统是否安全；网络应用是否安全；网络管理是否安全。



10.4.1　网络的物理安全风险

网络的物理安全主要是指：地震、水灾、火灾等环境事故；电源故障；人为操作失误或错误；设备被盗、被毁；电磁干扰；线路截获；高可用性的硬件、双机多冗余的设计、机房环境及报警系统、安全意识等。它是整个网络系统安全的前提，在企业区局域网内，由于网络的物理跨度不大，只要制定健全的安全管理制度，做好备份，并且加强网络设备和机房的管理，这些风险是可以避免的。

10.4.2　网络平台的安全风险

网络结构的安全涉及网络拓扑结构、网络路由状况及网络的环境等。现代企业局域网内公开服务器区(FTP、WWW、E-mail 等服务器)作为公司的信息发布平台，一旦受到攻击不能运行，对企业的声誉影响巨大。同时公开服务器本身要为外界服务，必须开放相应的服务。每天，黑客都在试图闯入 Internet 节点，如果不保持警惕，可能连黑客怎么闯入这些节点的都不知道，甚至会成为黑客入侵其他站点的跳板。因此，规模较大网络的管理人员对 Internet 安全事故做出有效反应变得十分重要。有必要将公开服务器、内部网络与外部网络进行隔离，避免网络结构信息外泄；同时还要对外网的服务请求加以过滤，只允许正常通信的数据包到达相应主机，其他的请求服务在到达主机之前就应该遭到拒绝。

安全的应用往往是建立在网络系统之上的，网络系统的成熟与否直接影响安全系统成功的建设。在企业局域网络系统中，用作与 Internet 连接的边界路由器，网络结构相对简单，具体配置时可以考虑使用静态路由，这就大大减少了因网络结构和网络路由造成的安全风险。

10.4.3　网络系统的安全风险

显而易见，系统的安全是指整个局域网网络操作系统、网络硬件平台是否可靠且值得信任。对于我国来说恐怕没有绝对安全的操作系统可以选择，无论是 Microsoft 的 Windows NT 还是其他任何商用 UNIX 操作系统，其开发厂商必然有其后门。可以这样讲，没有完全安全的操作系统，但是可以对现有的操作平台进行安全配置，对操作和访问权限进行严格控制，以提高系统的安全性。因此，不但要选用尽量可靠的操作系统和硬件平台，而且必须加强登录过程的认证(特别是在到达服务器主机之前的认证)，确保用户的合法性；其次应该严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。

10.4.4　应用服务的安全风险

应用系统的安全与具体的应用有关，它涉及很多方面，应用系统的安全是动态的、不断变化的，应用的安全性也涉及信息的安全性。应用的安全涉及面很广，以目前 Internet 上应用最为广泛的 E-mail 系统来说，其解决方案有几十种，但其系统内部的编码甚至编译器导致的 BUG 是很少有人能够发现的，因此一套详尽的测试软件是必需的。但是应用系统是不断发展且应用类型是不断增加的，其结果是安全漏洞也是不断增加且隐藏得越来越深。因此，保证应用系统的安全也是一个随网络发展不断完善的过程。



应用的安全性涉及信息、数据的安全性，信息的安全性涉及机密信息泄露、未经授权的访问、破坏信息完整性、假冒、破坏系统的可用性等。对于有些特别重要的信息需要对内部进行保密的(如领导子网、财务系统传递的重要信息等)，可以考虑在应用级进行加密，针对具体的应用直接在应用系统开发时进行加密。

10.4.5　网络信息管理的安全风险

管理是网络中安全最重要的部分，责权不明、管理混乱、安全管理制度不健全及缺乏可操作性等都可能引起管理安全的风险。当网络出现攻击行为或网络受到其他一些安全威胁时(如内部人员的违规操作等)，无法进行实时的检测、监控、报告与预警。同时，当事故发生后，也无法提供黑客攻击行为的追踪线索及破案依据，即缺乏对网络的可控性与可审查性。这就要求必须对站点的访问活动进行多层次的记录，及时发现非法入侵行为，建立全新网络安全机制，必须深刻理解网络并能提供直接的解决方案，因此，最可行的做法是管理制度和管理解决方案的结合。

10.4.6　人为的网络信息安全问题

1. 通用网关接口(CGI)漏洞

有一类风险涉及 CGI(Common Gateway Interface)脚本、许多页面文件和指向其他页面或站点的超链接，然而有些站点用到这些超链接所指站点寻找特定信息。搜索引擎是通过 CGI 脚本执行的方式实现的，黑客可以修改这些 CGI 脚本以执行他们的非法任务。通常，这些 CGI 脚本只能在这些所指 WWW 服务器中寻找，但如果进行一些修改，他们就可以在 WWW 服务器之外进行寻找。要防止这类问题发生，应将这些 CGI 脚本设置为较低级用户特权，提高系统的抗破坏能力，提高服务器备份与恢复能力，提高站点内容的防篡改与自动修复能力。

2. 恶意代码的攻击

计算机病毒一直是计算机安全的主要威胁，能在 Internet 上传播的新型病毒以及病毒的种类和传染方式也在增加，国际空间的病毒总数已达上万甚至更多。当然，查看文档、浏览图像或在 Web 上填表都不用担心病毒感染，然而，下载可执行文件和接收来历不明的 E-mail 文件需要特别警惕，否则很容易使系统遭到严重的破坏。

3. 对计算机网络的攻击

一般认为，目前对网络的攻击手段主要表现在以下几个方面。

(1)　非授权访问。没有预先经过同意，就使用网络或计算机资源被看作非授权访问，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。它主要有假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。

(2)　信息泄露或丢失。它指敏感数据在有意或无意中被泄露出去或丢失。它通常包括：信息在传输中丢失或泄露(如“黑客”利用电磁泄漏或搭线窃听等方式可截获机密信息；通过对信息流向、流量、通信频度和长度等参数的分析，推出有用信息)，信息在存储介质中


丢失或泄露，通过建立隐蔽隧道等窃取敏感信息。

(3)　破坏数据完整性。以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加，修改数据，以干扰用户的正常使用。

(4)　拒绝服务攻击。它不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

(5)　利用网络传播病毒。通过网络传播计算机病毒，其破坏性大大高于单机系统，而且用户很难防范。

复习思考题十

1. 简述需求分析的意义。
2. 现代企业网络信息安全的总体设计应从哪些方面考虑?
3. 网络信息安全制度的意义是什么?

参 考 文 献

[1] 贾铁军. 网络安全实用技术[M]. 北京：清华大学出版社，2011.
[2] 刘远生. 计算机网络安全[M]. 北京：清华大学出版社，2006.
[3] 戚文静，刘学. 网络信息安全与应用[M]. 北京：中国水利水电出版社，2005.
[4] 杨富国. 网络设备安全与防火墙[M]. 北京：清华大学出版社；北京交通大学出版社，2005.
[5] 石淑华，池瑞楠. 计算机网络安全基础[M]. 北京：人民邮电出版社，2005.
[6] 阎慧，王伟，宁宇鹏等. 防火墙原理与技术[M]. 北京：机械工业出版社，2004.
[7] 陈明. 网络安全教程[M]. 北京：清华大学出版社，2004.
[8] 顾巧论，高铁杠，贾春福等. 计算机网络安全[M]. 北京：清华大学出版社，2004.
[9] 黄传河等. 网络安全[M]. 武汉：武汉大学出版社，2004.
[10] 李仁发. 计算机网络安全[M]. 北京：科学出版社，2004.
[11] 阙喜戎，孙悦，龚向阳等. 信息安全原理与应用[M]. 北京：清华大学出版社，2004.
[12] 牛少彰. 信息安全概论[M]. 北京：北京邮电大学出版社，2004.
[13] 徐国爱. 网络安全[M]. 北京：北京邮电大学出版社，2004.
[14] 万振凯，苏华，韩清. 网络安全与维护[M]. 北京：清华大学出版社，2005.
[15] 荆继武. 信息安全技术教程[M]. 北京：中国人民公安大学出版社，2007.
[16] 陈建伟. 计算机网络与信息安全[M]. 北京：中国林业出版社，2006.
[17] 赵春晓. 计算机网络管理案例教程[M]. 北京：清华大学出版社，2010.
[18] 刘荫明. 计算机安全技术[M]. 北京：清华大学出版社，2002.
[19] 谢冬青. 计算机网络安全技术教程[M]. 北京：清华大学出版社，2007.
[20] 蔡红柳. 信息安全技术及应用实验[M]. 北京：科学出版社，2004.